NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

ROLE-BASED ACCESS CONTROL FOR COALITION PARTNERS IN MARITIME DOMAIN AWARENESS

by

Christopher R. McDaniel
Matthew L. Tardy

June 2005

Thesis Advisor:	James B. Michael
Co-Advisor:	Alan A. Ross

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** June 2005	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Role-Based Access Control for Coalition Partners in Maritime Domain Awareness			**5. FUNDING NUMBERS**
6. AUTHOR(S) **Christopher R. McDaniel** **Matthew L. Tardy**			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) Naval Postgraduate School CDTEMS Program Monterey, CA 93943-5000			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**
13. ABSTRACT (maximum 200 words) The need for Shared Situational Awareness (SSA) in accomplishing joint missions by coalition militaries, law enforcement, the intelligence community, and the private sector creates a unique challenge to providing access control. In this thesis we investigate the capabilities and limitations of Role-Based Access Control (RBAC) to control the dissemination of SSA in a coalition environment. Our case study is that of controlling access to SSA in the Maritime Domain Awareness (MDA) environment. MDA exemplifies both rapid change in membership of coalitions and the roles of coalition participants. We explore the access policy and roles played by the participants in the MDA environment, in addition to the characteristics of those roles. We make use of feasible scenarios to provide us with a base for applying models to the situation. The models that are applied to the scenario provide the formal methods that prove that RBAC policies and derivatives such as Distributed Role Based Access Control (DRBAC), Coalition Based Access Control (CBAC) and Temporal Role Based Access Control (TRBAC) can be used in conjunction with the Information Broker (IB) concept to provide adequate access control policies.			
14. SUBJECT TERMS Access control, computer security, homeland defense, homeland security, maritime domain awareness, Role-Based Access Control, RBAC, shared situational awareness, SSA			**15. NUMBER OF PAGES** 108 **16. PRICE CODE**
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

ROLE-BASED ACCESS CONTROL FOR COALITION PARTNERS IN MARITIME DOMAIN AWARENESS

Christopher R. McDaniel
Captain, United States Army
B.A., North Carolina Wesleyan College, 1993

Matthew L. Tardy
Lieutenant, United States Navy
B.S., University of Illinois, 1998

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
June 2005

Authors: Christopher R. McDaniel
Matthew L. Tardy

Approved by: Professor James B. Michael
Thesis Advisor

Professor Alan A. Ross
Co-Advisor

Professor Peter J. Denning
Chairman, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The need for Shared Situational Awareness (SSA) in accomplishing joint missions by coalition militaries, law enforcement, the intelligence community, and the private sector creates a unique challenge to providing access control. In this thesis we investigate the capabilities and limitations of Role-Based Access Control (RBAC) to control the dissemination of SSA in a coalition environment. Our case study is that of controlling access to SSA in the Maritime Domain Awareness (MDA) environment. MDA exemplifies both rapid change in membership of coalitions and the roles of coalition participants. We explore the access policy and roles played by the participants in the MDA environment, in addition to the characteristics of those roles. We make use of feasible scenarios to provide us with a base for applying models to the situation. The models that are applied to the scenario provide the formal methods that prove that RBAC policies and derivatives such as Distributed Role Based Access Control (DRBAC), Coalition Based Access Control (CBAC) and Temporal Role Based Access Control (TRBAC) can be used in conjunction with the Information Broker (IB) concept to provide adequate access control policies.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACL	Access Control List
BAP	Broker Architectural Pattern
CDO	Command Duty Officer
CIA	Central Intelligence Agency
CIP	Common Intelligence Picture
COP	Common Operational Picture
CBAC	Coalition Based Access Control
CTU	Counter Terrorism Unit
DAC	Discretionary Access Control
DEA	Drug Enforcement Agency
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DRBAC	Distributed Role-Based Access Control
ELINT	Electronic Intelligence
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FIST	Field Intelligence Support Team
GUI	Graphical User Interface
IB	Information Broker
ICE	United States Immigration and Customs Enforcement
IWO	Intelligence Watch Officer
MAC	Mandatory Access Control

MDA	Maritime Domain Awareness
MIFC	Maritime Intelligence Fusion Center
MIO	Maritime Interception Operations
MLS	Multi Level Security
MSO	Marine Safety Office(r)
NCW	Network Centric Warfare
NGO	Non Government Organization
NIST	National Institute of Standards and Technology
NORTHCOM	United States Northern Command
NYPD	New York Police Department
PACOM	Pacific Command
PANYNJ	Port Authority of New York and New Jersey
PKI	Public Key Infrastructure
RAB	Role Activation Base
RBAC	Role-Based Access Control
RBAC	Role-Based Access Control
SCI	Sensitive Compartmented Information
SIGINT	Signals Intelligence
SIPRNET	Secret Internet Protocol Router Network
SSA	Shared Situational Awareness
STRATCOM	United States Strategic Command
TAO	Tactical Action Officer

TENCAP	Tactical Exploitation of National Capabilities
TRBAC	Temporal Role-Based Access Control
USCBP	United States Customs and Border Protection
USCG	United States Coast Guard
USN	United States Navy
WEBTAS	Web Temporal Analysis System
WMD	Weapons of Mass Destruction

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

We would like to thank Professor Bret Michael and Professor Alan Ross for serving as our advisors and providing us with guidance and direction in the development of our thesis. We would like to thank Professor Ross for introducing us to the Maritime Domain Awareness group at the Naval Postgraduate School and giving our thesis a direction. We would like to offer additional gratitude and respect to Professor Michael who helped us develop a better understanding of computer security policies and how to develop them. His constant encouragement and valuable discussions were invaluable as our research progressed. His remarkable expertise in conducting research and in writing, particularly when combined with his willingness to share them with students, is a testament to his dedication as an educator.

We are also greatly appreciative to Professor Duminda Wijesekera of George Mason University for his insightful comments, suggestions and technical expertise on role-based access controls.

We would like to thank Mr. Scott Blatter and Lieutenant Michael Bennett, USCG, of the Coast Guard Maritime Intelligence Fusion Center for showing us the USCG operations center and providing some needed direction in our ongoing research. We would like to thank Mr. Fred Glasear and all the folks down at Maxim Corporation for sharing their research and helping us focus our efforts on realistic scenerios.

Most of all, we are grateful to our wives and children for supporting us for the last two years. Our families are what kept us balanced and grounded in reality when we occasionally spent too much time in front of a computer or reading obscure textbooks. Thanks for keeping us sane.

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

The need for Shared Situational Awareness (SSA) in accomplishing joint missions by coalition militaries, law enforcement, the intelligence community, and the private sector creates a unique challenge to providing access control. In this thesis we investigate the capabilities and limitations of Role-Based Access Control (RBAC) to control the dissemination of SSA in a coalition environment. Our case study is that of controlling access to SSA in the Maritime Domain Awareness (MDA) environment. MDA exemplifies both rapid change in membership of coalitions and in the roles of coalition participants. We explore the access policy and roles played by the participants in the MDA environment, in addition to the characteristics of those roles.

The CG MIFC and the Navy TENCAP project Radiant Alloy supplied valuable advice and data in the development of scenarios for the case studies. The models that are applied to these scenarios provide the formal methods that prove that RBAC policies and derivatives such as Distributed Role Based Access Control (DRBAC), Coalition Based Access Control (CBAC) and Temporal Role Based Access Control (TRBAC) can be used in conjunction with the Information Broker (IB) concept to provide adequate access control policies.

We determined that an interlinking between RBAC (and its derivatives) and Information Brokers is not only possible, but also highly desirable. Elements of DRBAC and CBAC are most suitable for alignment with the Information Broker, especially when designing a system for coalition use. It is scalable to large data sets and can include large quantities of entities and roles. DRBAC is especially useful for coalition environments in that it can limit information to members that have lower clearances or when combined with an information broker, it can prevent knowledge of the source of the data which is equally important.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. OVERVIEW

The purpose of this thesis is to assess the feasibility of applying a Role Based Access Control (RBAC) policy (or a derivative of it) onto the Maritime Domain Awareness (MDA) project using case studies and formal methods. Additionally, this thesis will explore the tenants of the Information Broker and the Radiant Alloy program and how they may relate or assist in the MDA program. Finally, this thesis will assess the feasibility of the benefits of RBAC assisting in the development of the Radiant Alloy program. The policies, project, and program mentioned above will be discussed in further detail later in this thesis.

This chapter will first provide background information on MDA, the Information Broker, Radiant Alloy, and a brief discussion on sensor networks. Next, this chapter will discuss Shared Situational Awareness and how the different actors play roles in providing and using information to create a common operating picture, thus providing all users with the most accurate an up-to-date information. RBAC, Distributed Role Based Access Control (DRBAC), Coalition Based Access Control (CBAC), and Temporal Role Based Access Control (TRBAC) will work together to control this access and is the focal point of this thesis. The final section of this chapter will provide a brief introduction to the rest of the paper.

B. BACKGROUND

This thesis addresses the challenge of providing access control in a coalition setting in which membership in the coalition and the roles are in constant flux. The scope of this thesis is limited to an investigation of the application of Role-Based Access Control (RBAC) for Maritime Domain Awareness (MDA). MDA is concerned with maintaining a worldwide common intelligence picture (CIP) of maritime traffic via a distributed network of intelligence, surveillance, and reconnaissance (ISR) systems.

MDA supports Maritime Domain Protection (MDP), which involves the use of MDA to safeguard the security of the U.S. and its allies.

> MDA spans dozens of issues – from missile defense and counterterrorism to cargo and container security, from drug trafficking and immigration to fishing rights and search and rescue.[1]

Numerous government and non-government entities are participating in MDA. Within the United States, the MDA effort has to date been spearheaded by the Department of Homeland Security, the Coast Guard, and Navy. MDA is not a completed solution, but an ongoing project aimed at solving the complex problems defined throughout the following sections.

1. Maritime Domain Awareness

The main goal of MDA is to identify, monitor, and track vessels as they approach the maritime borders of the United States. Knowing where they have been, what they are carrying, where they have stopped and tracks they have taken to get there will aid in preventing a terrorist attack. The United States cannot search and inspect every piece of cargo that enters the United States, so we must perform risk-based decision making with data gathered from our sources.[2] The United States must be able to abstractly push out our maritime borders in order to provide our assets with more time to make decisions and search vessels of interest and must possess awareness of vulnerabilities from the water and related threats: this must be done without disrupting the lawful and legitimate commercial traffic that transits through international and US territorial waters.

The threats the United States faces at its maritime borders are similar to threats at other points of entry. We must protect ourselves from people, cargo, and the vessels themselves.[3] Implementing MDA will help protect our borders from these threats. MDA involves the collection, processing, and evaluation of large amounts of data from a wide

---

[1] Johns Hopkins University Applied Physics Laboratory Web Site. Available from <http://www.jhuapl.edu/newscenter/aplnews/2004/summer_MDA.htm> (accessed 19 September 2004).

[2] Vice Admiral Thomas H. Collins. United States Naval Institute Speech. April 3, 2002. Available from <http://www.uscg.mil/COMMANDANT/Maritime%20Security%20Plan%20USNI%20040302.htm> (accessed 19 September 2004).

[3] Vice Admiral Thomas H. Collins.

spectrum of sources. The data must be fused and given security labels and markings before it can be disseminated to government and non-government organizations (NGOs). Each particular government organization or NGO will have personnel with different needs for access to the CIP. Due to the fact that the CIP will be maintained in distributed electronic repositories, there needs to be computer security mechanisms in place to broker access to the contents of the repositories. There is a time value associated with each piece of data contained in the CIP repositories, so the access-control and other dissemination mechanisms must be consistent with the time-budget requirements for accomplishing the MDP mission.

2. Maritime Domain Awareness at NPS

The Maritime Domain Awareness research initiative at the Naval Postgraduate School is concerned with possible courses of action with regards to maritime terrorism. There are numerous research projects underway at NPS including Command and Control, Port Security and Infrastructure, data tagging and data fusion, and systems design and multi-level security. Our thesis addresses the issue of access control to the open-source and possibly data repositories comprising the MDA CIP. In the course of our research, we met with representatives from the Maritime Intelligence Fusion Center (MIFC) located in Alameda, California and with representatives from the Navy Tactical Exploitation of National Capabilities Program (TENCAP) to investigate the possibility of employing Role-Based Access Control (RBAC) to serve as a means for protecting the confidentiality and integrity of the MDA CIP. Although multilevel security (MLS) is a major focus within the TENCAP program, we chose to limit the scope of our thesis to investigating the application of RBAC to MDA. We do, however, offer a discussion within the thesis of MLS issues as they pertain to the application of RBAC to MDA

3. MDA and the Coast Guard

While visiting MIFC, we were provided with a copy of a document entitled “Defining a Common Intelligence Picture for the United States Coast Guard: A Port

Perspective."[4] The document contains a description of roles and positions within MDA and the process that occurs when tracking and boarding suspect vessels. The following question is addressed within the document: What policies, relationships, and information flow processes must be in place in order to develop a CIP supporting MDA for any given Coast Guard captain of the port's area of responsibility (AOR)? The author of the document recommended that the information gap be bridged between the various parties, operating in different administrative domains and under different legal authority, in order to maintain and utilize the MDA CIP. Members of the Radiant Alloy Project are developing a system to manage the CIP and other resources via automated information brokers. In our thesis we explore RBAC in the context of information brokering.

4. Information Broker

The Information Broker is an information-management service that will act as an intermediary between the requester of the information and the data repository. The IB will provide the requester with the data and at the same time, shield the source of that data from the requester. It is a black-box approach that will satisfy the data requests and protect the source. The IB must be able to deal with a myriad of clearances and classified data. It may range from unclassified all the way to the highest Top Secret Compartmented Information. Additionally, there will be users of the system who have the full range of United States clearances but it must also provide information to allied nations or even to non-government organizations. Within the context of this thesis, there are two proposed modes in which the Information Broker utilizes RBAC. The primary mode for the Information Broker is to be the intermediary through which the data is specifically requested by the user. This is the concept this thesis will use during the modeling stage. The other mode that is not explicitly used in the models is the automatic piping mode. Data is automatically sent to roles fitting a certain approved profile.

5. RBAC and Radiant Alloy

One of the objectives of the Radiant Alloy Project is to develop operational views of an information broker strategy that will enable TENCAP to achieve certification and

[4] Lieutenant Michael E. Bennett. Defining a Common Intelligence Picture for the United States Coast Guard: A fPort Perspective. (Joint Military Intelligence College, August, 2003).

accreditation for MDA-CIP-type systems at Protection Level (PL) 5.[5] The information broker (IB) serves as an information-management service: it acts as an intermediary between the requester (or consumer) of data and the producer or repository of data. The IB provides the requester with the data and at the same time, shields the source of that data from the requester. The IB must manage access to the data in repositories, both by classification level and compartment. More broadly speaking, an information broker is the key component of the Broker Architectural Pattern (BAP). The BAP is intended to be used to structure distributed software systems with unlinked mechanisms that interact by remote service invocations. The broker component is responsible for coordinating communication, such as forwarding requests, as well as transmitting results and exceptions.

MDA has the requirement to provide information across domains, to include entities such as government organizations and NGOs. Further, access to data repositories must be simple and efficient, but provide for local as well as coalition-based enforcement of access-control policy. Radiant Alloy is a tool that attempts to solve this problem. It could be used to support military, humanitarian, law enforcement, and intelligence missions. Within Radiant Alloy, RBAC provides a mechanism for managing access permissions by way of roles that users play, rather than on a user-by-user basis. Each IB within MDA can have its own RBAC policy, as well as Meta rules for managing RBAC policy updates and enforcement between Information Brokers.

6. MDA Information Broker and Sensor Networks

The chain of events that lead up to a user accessing data in a repository starts with sensors. Sensors and human intelligence (HUMINT) provide the raw data that is eventually turned into useable information. Sensors are remote, proximal, or in situ and MDA will mostly deal with the first two. In situ sensors, or sensors that are right there in close proximity to their destination, are not too important within MDA. Sensors also have different levels of classification and there will be situations in which the overseeing

---

[5] Director of Central Intelligence Directive 6/3. *Protecting Sensitive Compartmented Information within Information Systems*. (June 1999).

authority does not want the end user to know where the data came from. The path between the data source and the data sink must not be known. For example, if there is satellite coverage provided by the National Reconnaissance Office (NRO) that is classified Top Secret, that data is provided to the information broker who shields the NRO from being identified as the source of the data. The information brokering concept is also not a single, centralized repository. It consists of many data sources communicating via many Information Brokers and sharing data. For example, if a user requests information that is not accessible through any of the Information Brokers that the organization uses, IB's have the capability to query other IB's for the requested data. The data would then be processed through the secondary IB back through the organization IB and to the user. The term secondary information broker does not mean that it is a less privileged secondary clearinghouse for information, but simply another IB that is not the user's primary information broker (see Figure 1). Any Information Broker can be either primary or secondary, depending on the source of the data request.

The MDA system is an event-driven system-of-systems. Part of that system-of-systems is a distributed network of heterogeneous sensors. The owners of the sensors—U.S. and foreign governments, non-government organizations, and private industry--each have their own level of security labels and have sensors or sources that may be classified or controlled in some manner. In any case, what is important is that the data gets to the right user (or role) so that it can be processed and appropriate action can be taken. It does not make sense for the user to go directly to the sensor's repository to gather the information, but to go to the user's own repository to query for that data. It is also beneficial for the user to 'sign up' for updates of interest to the user to be delivered automatically; this can be done through the use of user profiles and database triggers. It is unreasonable to expect the sensor repositories to do this. It will be the job of the information broker to provide the updates as they happen or to query the appropriate secondary information broker. The Information Broker can poll the sensor repository or receive updates based on the occurrence of events; the update method should be transparent to the end user. Using RBAC, the administrator can establish data attributes

for the user and extend those attributes to meet data classification types and gain access to the data that the user needs to carry out the mission at hand.

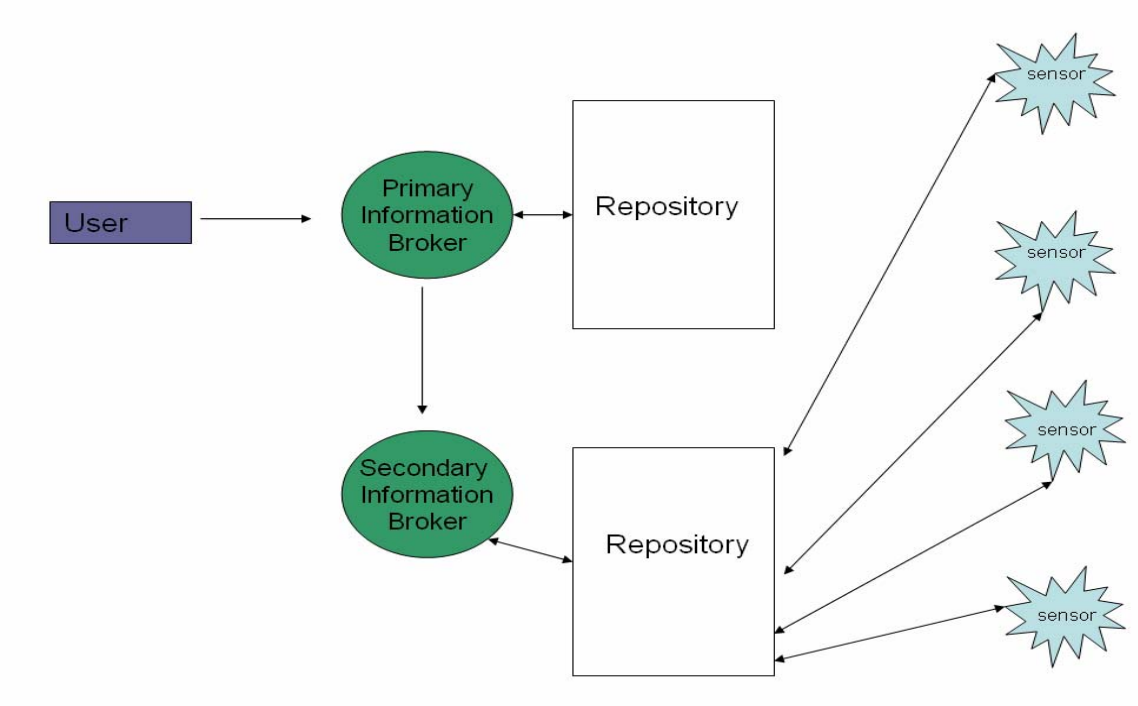

Figure 1. Information Broker with Sensor Network

C. SHARED SITUATIONAL AWARENESS

The need for Shared Situational Awareness (SSA) among coalition militaries, law enforcement, intelligence, and private sectors creates a unique problem within access control. There is a need for SSA within MDA because of the vast quantity of data and intelligence that could be fused to track ships and their cargo. The multitude of agencies involved require up-to-date and correct information to best coordinate actions and interdiction, ultimately protecting the security of the United States and its allies. In this thesis we investigate the pros and cons of relying on RBAC to control access by members

of coalitions to SSA; the term "coalition" is used in this thesis to include all of the organizations that are or could be involved in conducting MDA, including militaries, law enforcement agencies, nongovernmental organizations, private industry, and foreign governments. Both the membership within coalitions and the roles of all participants can be fluid. Thus, it is necessary to be able to adjust access to SSA data accordingly. We use a case-study approach to gain an understanding of the MDA environment and the requirements for SSA. We then turn our attention to exploring the access policy and roles played by the participants in the MDA environment, in addition to the characteristics of those roles (e.g., the frequency and magnitude of change, the differences between roles across administrative domains, and Meta roles). For example, there can be many organizations and roles within the organizations for which accessing views of the operational picture of New York Harbor will be necessary. However, a role defined within the Port Authority of New York and New Jersey (PANYNJ) or the New York Police Department (NYPD) may have the same name but different responsibilities (including need-to-know for data sharing) and the access policies between PANYNJ and NYPD may differ at any point in time. How do we address non-equivalence of roles and inconsistencies in policies across administrative domains? Can we enforce RBAC policy across administrative domains? Does RBAC help us here? We will try to answer these and other related questions

D. RBAC ACTORS

RBAC provides a means to simplify management of access control to shared objects within information systems. In the past, access control was managed on a user-by-user basis. RBAC policy relies on explicit definition of roles that users of an information system play in an organization; that is, access to shared objects is associated with roles (e.g., "tactical action officer"), not individual users ("LCDR Smith"). Users gain access to data based on their current role. A role can be defined by position, rank, authority, responsibility, or leader. It may be a generic role or a specific position. This role can then be mapped to accepted universal standards. Accordingly, different coalition members and their organizations (e.g., law enforcement, military, intelligence, NGO,

shipping companies, port authorities) could also be mapped to the same standards, allowing them to share as well as access data they need. To accomplish this, we have chosen three categories of actors that must be defined: Intelligence, Law Enforcement and Military. An actor is any individual or group participating in a specific activity related to the current operation. Specific roles within these categories will be defined in scenarios later in this thesis.

1. Domestic Categories of Actors

a. Intelligence

Intelligence focuses on information gathering, analysis, and dissemination about potential threats. This data will be used by both homeland defense and homeland security personnel to determine boarding requirements.[6]

b. Law Enforcement

Law enforcement accesses entry and exit data and takes appropriate actions on foreign nationals who have overstayed their legal duration. Law Enforcement is utilized to prevent, investigate, apprehend or detain individuals suspected of breaking laws that fall within the realm of MDA. Law enforcement encompasses a wide range of agencies including, but not limited to, local police, FBI, Drug Enforcement Agency, United States Customs and Border Protection and the United States Coast Guard.

c. Military

Military assets work with the Department of Homeland Security and various American federal agencies in identifying, tracking, interdicting, and/or boarding targets of interest.

2. Foreign Categories of Actors

a. Intelligence

While working with domestic intelligence, foreign intelligence provides data on potential targets of interest as they depart foreign countries. They work closely

---

[6] Homeland defense refers to the military aspect of protecting the homeland in addition to intelligence activities conducted against non-U.S. persons, whereas homeland security encompasses the use of law enforcement and intelligence resources to protect the homeland.

with domestic intelligence to provide information that will be used to determine ships of interest.

b. Law Enforcement

Law enforcement accesses entry and exit data and takes appropriate actions on foreign nationals who have overstayed their legal duration. Apprehends individuals placed on watch lists.

c. Military

Military assets work with the Department of Homeland Security and various foreign governments/agencies in identifying, tracking, interdicting, and/or boarding targets of interest.

3. Private Categories of Actors

a. International Shipping.

International shipping will help in self identification and possibly contribute to intelligence gathering.

b. Transportation Industries

Transportation industries (air, sea or rail) will update entry and exit data on foreign nationals and uses watch lists to prevent entry to terrorists. Transportation industries will also notify appropriate law enforcement agencies upon identification of any individual who has been placed on a watch list.

c. Non-government Organizations (NGO)

> A non-governmental organization is an organization which is not part of a government. Although the definition can technically include for-profit corporations, the term is generally restricted to social and cultural groups, whose primary goal is not commercial.[7]

NGO's provide passive intelligence gathering on potential threats based on local knowledge and contacts in their area of operation.

---

[7] Wikipedia.org. <http://en.wikipedia.org/wiki/Non-governmental_organization> (accessed 12 April 2005).

E. RBAC POLICY ENGINE

The scope of our thesis is the application of RBAC within an MDA structure to support access control in a dynamic coalition environment. Figure 2 shows how actors interlink to provide Shared Situational Awareness in a coalition environment.

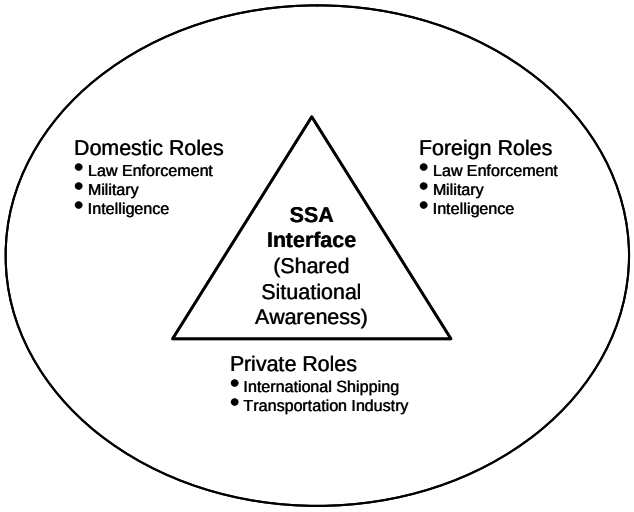

Figure 2. Actors and SSA

An interdiction chain is a progressive set of methodical steps used to counter potential threat-ships (see Figure 3). We first address the problem, then provide analysis of the problem and domain, and lastly take that data and put it into a model called Distributed Role-Based Access Control for Dynamic Coalition Environments (DRBAC).[8]

---

[8] Eric Freudenthal, T. Pesin, L. Port, E. Keenan, and V. Karamcheti. *DRBAC: Distributed Role-based Access Control for Dynamic Coalition Environments*. In Proc. 22nd Int. Conf. on Distributed Computing Systems. (Vienna, Austria: 2-5 July 2002), 411.

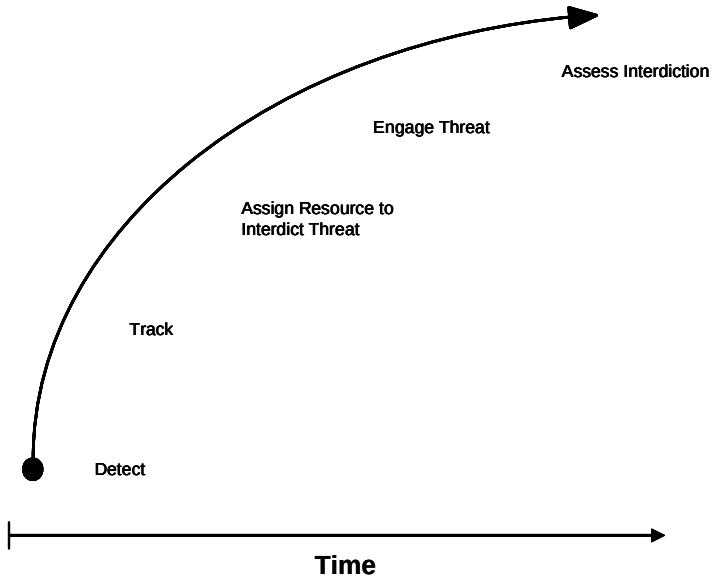

Figure 3. Interdiction Chain

F. SUMMARY

The background of MDA as examined throughout Chapter I has reinforced that it is not a completed solution, but an ongoing project. The entire scope of MDA (including its current state as well as what it seeks to achieve) is much too broad a topic to consider within the confines of this thesis. For the purposes of this study a simplification of MDA is needed to supply a context in which to study RBAC, Information Brokers, Radiant Alloy, etc. as they might apply to MDA. To accomplish this we will view MDA as the active and complete system that it seeks to be. This supplies a context for the rest of the thesis by allowing references to MDA in the present tense.

As just stated, Chapter I provided an introduction and background on Maritime Domain Awareness, RBAC, Information Brokers and Radiant Alloy. Chapter II further explores different forms of RBAC and how it applies to MDA. Chapter III examines the

flow of data and roles in two sample case studies. Chapter IV continues the development of the case studies, and demonstrates a systematic formal approach showing that Role-Based Access Control can be done. Models are used to explain how it can be done and why it is appropriate for MDA. Chapter V details the results and contributions of the research. Chapter VI provides a summary of the thesis and recommendations for future research. A glossary is included in Appendix A with helpful definitions for the reader.

THIS PAGE INTENTIONALLY LEFT BLANK

II. RBAC AND MDA

A. ROLE-BASED ACCESS CONTROL

Let us start with a simple example to explore how RBAC can be used to support MDA. In our vignette, Spanish intelligence discovers that a commercial vessel embarked for the United States, allegedly loaded with a shipment of anthrax. Coalition RBAC (CBAC) is applied to the data repository and allows the Spanish intelligence community to input data about the potential threat into a data repository accessible via the MDA system. The ship has already departed, no track was filed, and the ship has been "lost." International shipping companies can access the downgraded data about the name of the ship and that it is on a watch list. They can make reports to law enforcement activities that the ship has been spotted. Once the ship has been located and tracked, data is entered into the data repository and U.S. Navy and Coast Guard personnel can access the data based on their current roles. For example, alerts are sent and the associated watch officers on board the Naval or Coast Guard ship can access data appropriate for the situation. It will not matter who they are but rather what roles they are playing. On board the Navy ship, when the watch is turned over, there is a seamless transition from one watch officer to the next. The same thing happens on the Coast Guard ship. The threat ship is tracked and approaches the continental United States. The Coast Guard had already been alerted and positions a cutter to prepare for a boarding. Other agencies, including local police and FBI agents need data related to cargo and crew names; this process has already begun. Access is granted to government personnel based on the roles they play. The tenants of Temporal Role-Based Access Control (TRBAC) can also be applied in this scenario. For instance, specific roles can be activated and deactivated based on situational requirements. Similarly, triggers can be applied that activate a role. For example, once local law enforcement has been notified via an alert, this would also trigger the activation of a federal law enforcement role such as an FBI watch officer.

RBAC is founded upon associating permissions with roles, and users are made members of roles. The genesis of RBAC can be traced to the emergence of multi-user and

multi-application on-line systems. The assignment and membership principle mentioned in the first sentence is central to simplifying the management of permissions; this would be applicable to MDA as it is not known whether the current multilevel security is the best way to administer a large collection of users and accesses. Traditional Discretionary Access Control (DAC)[9] and Mandatory Access Control (MAC)[10] may not provide the degree of agility required within the MDA program to update access-control policy. DAC policies, which allow users to control access to their own files, do not fit well into a role-defined system. MAC policies made by a system to control access to objects of different secrecy labels are also too rigid for the changing MDA coalition members. RBAC policies could adopt portions from each as necessary. The National Institute of Standards and Technology (NIST) concluded in 2001 that RBAC addresses the needs of many commercial and government organizations.[11]

RBAC also facilitates security administration and review. RBAC makes it possible to predetermine role-permission relationships, so that users can be assigned to predefined roles. The NIST study determined that permissions assigned to roles tend to change relatively slowly compared to changes in user membership roles. Assignment of users to roles requires less technical skill than assignment of permissions to roles, thereby simplifying the process. This would be beneficial to MDA because user membership roles may change often; for instance, there is typically a high turnover rate of military personnel. Additionally, more than one person can play the same role concurrently. Assigning qualifications and permissions to the roles would be easier than reevaluating each person every time the person's role changes. RBAC's relationship to MAC and DAC is fluid. RBAC is policy-neutral and can have either a MAC or a DAC flavor.

---

[9] DAC policies relies on the discretion of the owner of the file to dictate who has a need to know and can pass access to the object to other subjects.

[10] MAC policies protect objects by assigning sensitivity labels to those objects and comparing the labels to the level of sensitivity of a subject and grants access accordingly.

[11] D. Richard Kuhn, Chandramouli Ramaswamy, David F.Ferraiolo, Serban Gavrila, and Ravi Sandhu. *Proposed NIST Standard for Role Based Access Control.* ACM Transactions on Information and Systems Security. Volume 4, Issue 3. (New York: ACM Press, August 2001), 249.

The base model of RBAC includes a user, a role, a session, and permission. A user in this model is a human. A role is a job function or a duty within some organization. A tactical watch officer on a Coast Guard cutter would be an example of a role. A session occurs when a user activates some subset of roles that he or she is a member of. A permission is a particular mode of access granted to one or more objects in the system: they are always positive and confer the ability to the user to perform some action (e.g., read, write, or delete a specific data item or type of data). The RBAC model captures the following types of relationships: many-to-many permissions to role assignment and many-to-many users to role assignment. There is a function that maps each session to a single user. Each session also gets mapped to a set of roles.

Hierarchies are also a part of RBAC. They are used to structure roles to reflect an organization's line of authority and responsibility. They form a partial order relationship, which means they are reflexive (role inherits its own permissions), transitive, and anti-symmetric (redundant). The hierarchy ensures that we are not able to establish a session with any combination of roles resulting in escalated privileges.

B. FORMS OF DISTRIBUTED ROLE-BASED ACCESS CONTROL

Under the umbrella of Distributed Role-Based Access Controls (DRBAC), we will examine DRBAC concepts explored by Freudenthal et al. as well as a derivative form, Coalition-Based Access Control (CBAC).

> Distributed Role Based Access Control is a scalable, decentralized trust management and access control mechanism for systems that span multiple administrative domains.[12]

1. DRBAC

The need to share information and resources in a coalition environment led to the development of the DRBAC model. The term "coalition" refers to organizations or nations collaborating together in order to achieve a common goal. Coalition members

---

[12] Eric Freudenthal, T. Pesin et al., 411.

directly share their resources with other members without having to go through a third party. Using DRBAC to control resources raises three problems that must be overcome:

- There must be different levels of access to accommodate different organizational structures in coalition members
- Trusts must be tracked and monitored to allow for revocations
- There needs to be an automatic distribution of credentials to allow members of a coalition to establish trust relationships

"Traditional role-based access control systems depend upon a central trusted computing base administered by a single authority."[13] This methodology does not scale well to the potential size and complexity of coalition environments. DRBAC defines permissions in terms of roles within an organization. These roles can then be mapped to others within the same organization or to equivalent roles within coalition partners.

As with many other models, DRBAC employs a methodology similar to PKI to authenticate delegation certificates. However, DRBAC has three features that make it unique. Firstly, it allows coalition members (also called entities) to delegate roles created by another entity; this process (also called third-party delegation) provides for scalability. Second, scalar values can be assigned to modify access levels to a resource. The authority to assign these values can also be delegated. Finally, status updates can be pushed to other entities allowing outdated or invalid credentials to be revoked using delegation subscriptions.[14]

Delegations are published, validated, updated and revoked using DRBAC wallets. Wallets are similar in function to PKI certificates and can store many delegations (see Figure 3 for an example of a wallet).

---

[13] Eric Freudenthal, T. Pesin et al., 411.

[14] Eric Freudenthal, T. Pesin et al., 412-413.

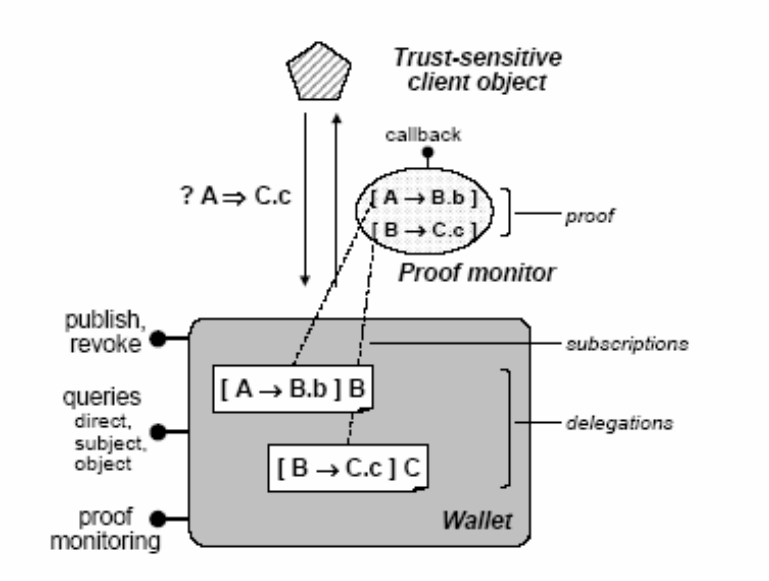

Figure 4. DRBAC Wallet[15]

Proof monitoring is an important concept within the wallet architecture. A proof monitor is a call back mechanism that provides for continuous monitoring of a trust relationship. When proof of a relationship is required, an entity can request a proof of a relationship through the proof monitor.[16] The concept of a proof monitor is closely related to the Information Broker idea. When verification of a relationship is required, the Information Broker can verify the trust relationship and determine if it is still valid. If it is not still valid, the relationship can be revoked or a further investigation commenced to verify the trust.

2. CBAC

Coalition Based Access Controls (CBAC) can be seen as an offshoot of DRBAC. It was designed to support the concept of secure sharing or resources between different organizations. Specifically, the goal of CBAC was to accurately capture inter-

---

[15] Eric Freudenthal, T. Pesin et al., 414.

[16] Ibid., 416.

organizational (coalition) relationships. Examples of some entities that might form coalitions include private businesses, government agencies, corporations, foreign governments, etc.

The inherent shortcoming of RBAC which led to the development of CBAC was that RBAC does not provide an abstraction to capture a set of collaborating users, operating in different roles which in our examples can be applied to coalition environments.[17] The entities which CBAC focuses on are Roles, Teams and Tasks. Within CBAC there are three key definitions:

- Role – a role captures a coherent aspect of an individual's job function within the organization.
- Team - a team is a collection of users assigned to various roles and working toward the accomplishment of a specific goal. The team definition specifies the roles that will be included within the team.
- Task – a task is a stateful flow of activities that achieve a particular function.

A key difference between DRBAC and CBAC is that CBAC makes use of abstract teams or tasks to create dynamic coalitions that are focused on completing a task or solving a problem. Coalition entities are formed or associated voluntarily and frequently on a temporal or temporary basis.

C. TEMPORAL ROLE-BASED ACCESS CONTROL

One can add a temporal dimension to RBAC. If someone is assigned a role that is only authorized to be accessed between certain times, the role should only be allowed activation during those times. This introduces a need to ensure dependencies are met as

---

[17] E. Cohen, R. K. Thomas, W. Winsborough, and D. Shands. *Models for Coalition-Based Access Control (CBAC).* In Proceedings of the Seventh ACM symposium on Access Control Models and Technologies. (Monterey, CA: ACM Press, 2002), 97-106. .

well. For example, a doctor on night duty may need a nurse on night duty.[18] In our MDA context, a night tactical watch officer on a Coast Guard cutter (0000-0600) may need to correspond with a night FBI watch agent.

TRBAC is an extension of the RBAC model and the main features are the possibility of periodically activating and deactivating a role and defining temporal dependencies. These dependencies can be activated by means of a role trigger, so that they are automatically executed based on current activations or deactivations of roles.

The RBAC model used in this paper is the same one proposed by Sandhu.[19] It consists of four basic components: a set of users, a set of roles, a set of permissions, and a set of sessions. When a user logs on, he creates a session. A user can be a member of many roles, and a role can have many members. For example, a watch officer on a cutter can stand officer of the deck and also Tactical Action Officer, for which different information is needed. Of course, a role (night watch) can have many members (the qualified watch standers). There is an assignment of a value of priority, high (H) or very high (VH) where H< VH, which would dictate the order of processing to ensure that the processes are scheduled according to the set temporal policy. An example is as follows: (RT_1 activate night cutter watch office -> (VH) activate night watch FBI.

RT_1 is a role trigger that states that 'night watch FBI' must be active if 'night cutter watch is active.' Additionally, roles with lower priorities, such as 'under instruction' watches can also be used.

A user requests to activate a role and is then permitted access if the user has authorization to play the role and the role is active at the time of request. In TRBAC, these roles can be immediately executed or deferred to a later time. Additionally, periodic

---

[18] Elisa Bertino, Elisa Pierro, Andrea Bonatti, and Elena Ferrari. *TRBAC: A Temporal Role Based Access Control Model.* Symposium on Access Control Models and Technologies. (Berlin, Germany: ACM Press, 2000), p 23

[19] R. S. Sandhu, E. J Coyne, H.L. Feinstein, and C.E Youman. *Role Based Access Control Models*. (IEEE Computer, Feb. 1996), 38-47.

events and role triggers are prioritized to deal with conflicting actions. Data maintained by the system are active roles, deferred actions, actions, events, and triggers.[20]

D. ATTRIBUTE BASED ACCESS CONTROL

Another form of access control that should be studied for its development of Meta rules is Attribute Based Access Controls (ABAC). ABAC grants accesses to services based on the attributes possessed by the requester. It can be used as a method of representing rules about rules (Meta rules). As opposed to DAC, ABAC uses sets of attributes in place of the *subjects*. Similarly it uses sets of services in the access control matrix in place of *objects*. This is useful in systems in which subjects (roles) are identified by their characteristics. In our model this is representative of role attributes that are substantiated by DRBAC wallets through Information Brokers. This is potentially the most important aspect of ABAC, in that it allows you to build different sets of rules which allow Information Brokers to work with each other. ABAC lets you manage the rules between the Information Brokers.

E. COMMAND AND CONTROL DISCUSSION

When employing a RBAC, one should not limit the response options of the participants in an MDA coalition. Data flow across the boundaries of administrative domains is an important facet to maximizing the benefits of a RBAC policy within MDA. As mentioned earlier, several organizations can be involved in an interception event. For instance, the Central Intelligence Agency (CIA) and the Defense Intelligence Agency (DIA) can coordinate with Navy, Coast Guard, local law enforcement, FBI, Federal Emergency Management Agency (FEMA), the Department of Homeland Security (DHS), or United States Strategic Command (USSTRATCOM) to align a proper response to a suspected threat. The level of coordination necessary among these organizations is determined by the quality and type of data gathered.

---

[20] Bertino et al., 21-30.

The collected intelligence goes through a three step process: collection, analysis, and dissemination. During the collection phase, intelligence is gathered by an agency. It is likely not very specific and may contain vast quantities of data. It has not been substantiated or assigned any likelihood of occurrence. No decision has been made as to what agency may require this data. That will occur during the next step, which is the analysis phase.

The intelligence gathered will be analyzed and a determination will be made as to the credibility of the threat, and who, what, where, when, why, and how will be attempted to be answered. Is the threat real? What kind of cargo might a suspicious ship be carrying? What is the nature of the threat? Is the suspicious ship carrying WMD or a missile pod or is there no threat at all? These questions will hopefully generate intelligence that will create a Shared Situational Awareness (SSA) among the agencies. If some of these questions can be answered, different agencies can be brought into the loop by unlocking certain roles within certain agencies within the MDA data repository. The data will be classified accordingly, further limiting access. The dissemination phase now begins where the intelligence is available to those agencies that need it. Decisions can now be made by appropriate agencies as to where and when the interception will occur. Will it happen in the open ocean? Will the Navy be doing open ocean Maritime Interception Operations (MIO)? Will it happen closer to shore where the Coast Guard will conduct MIO? The key would be to make every attempt to ensure that the United States is not forced into a bad decision as to where and when the boarding will occur, but that the decision is made after an analysis of all the available intelligence. Therefore, the data must flow through the collection, analysis, and dissemination process quickly and efficiently providing the necessary authorities with the required and correct intelligence to make a timely and informed decision. Network Centric Warfare involving all elements of the battle space and developing speed of command within our forces will play a major role in conducting a timely and effective interception operation. [21]

---

21 Vice Admiral Arthur K. Cebrowski and John J. Garstka. Network-Centric Warfare: Its Origin and Future. Proceedings of the Naval Institute. January, 1998. <http://www.usni.org/Proceedings/Articles98/PROcebrowski.htm> (accessed on 12 October 2004).

Consider the effects of RBAC on a command and control structure. TRBAC, CBAC and DRBAC are not policies, but rather variations on the base RBAC model. These models can be used to create access control policies that can be applied to facilitate quick access to the data by required actors, greatly improving command and control.

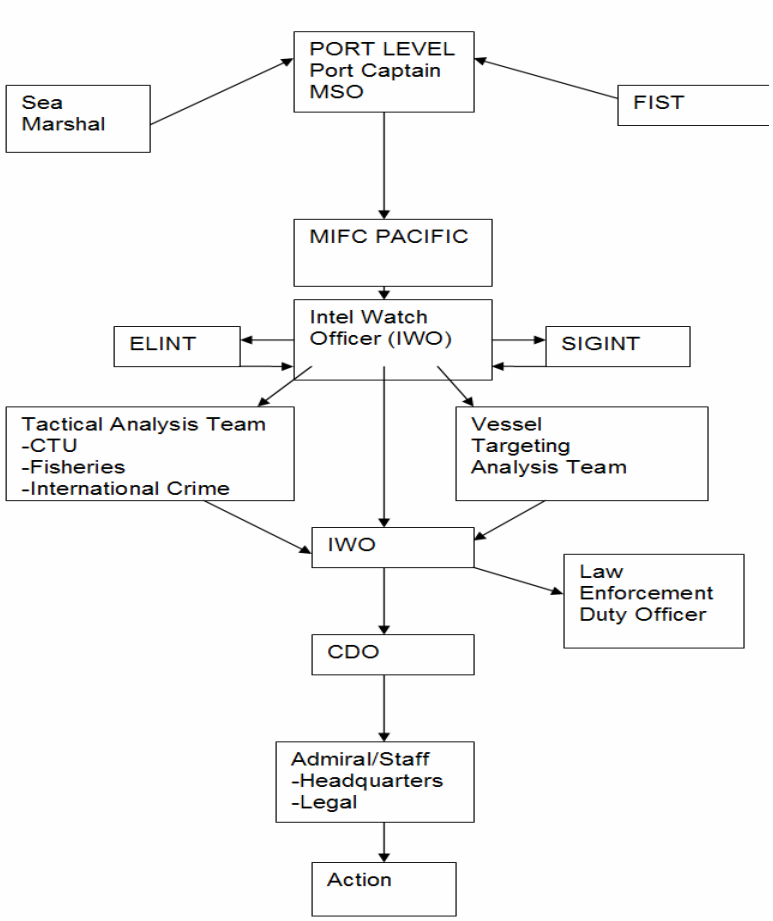

Figure 5. Coast Guard MIFC Organizational Chart

Figure 5 portrays the basic flow of intelligence and data from a ground up approach. This diagram was created with information gathered from a visit to the Maritime Intelligence Fusion Center at Coast Guard Island in Alameda, California. Even

a brief glance at the diagram will provide the reader with an idea of how many roles are played within a MDA activity. The system itself must be able to contain information classified up to the highest level but must also be able to disseminate intelligence down to the lowest possible level. The Information Broker concept could come into play in many different ways: a means for disseminating data via role or user-based profiles; a means for controlling access to data within an administrative domain; and a means to control access to data that crosses administrative domains.

The Information Broker as described in the Concept of Operations for Radiant Alloy must be able to perform this while protecting its information from untrained, uncleared, or malicious users. Data must be able to be exchanged across domains and security boundaries within the Information Broker scheme. The Information Broker must protect and disseminate at the same time. RBAC can be applied to the Information Broker in order to manage, distribute, and enforce policies inherent within them. Additionally, roles can be added and managed by one central Information Broker. Roles can be created for circumstances and deleted. Data can be shared with allied foreign governments or not shared based on levels of trust. Data can be shared with other agencies including local law enforcement, the Coast Guard, Drug Enforcement Agency, and even non-government organizations based on need to know. Policies can be written by the main Information Broker and disseminated to local brokers where they will be enforced and managed. There are RBAC models based on time, coalitions, and distribution.

In the preceding example, there could be many organizations that branch off of the initial report. Local and federal law enforcement would become involved if crime or attempted terrorism was suspected. If the cargo was determined to be dangerous to civilians in the area, FEMA and other disaster relief organizations may need to be in the loop. Every role, however, would not necessarily need all the data that is available. Only that which would allow them to do their jobs would be disseminated. This is where the Information Broker and RBAC can be utilized.

The roles in the Coast Guard example above are many. The legal staff, for example, plays a specialized Information Broker between different types of roles, law enforcement and defense of the homeland. Data may be forced to travel through a specialized data repository and determine which area it applies to. Is it a law enforcement role? When does it shift from defense to law enforcement? These decisions would need to be made by a legal expert.

WEBTAS (Web Temporal Analysis System) is a system in use by the Coast Guard and can be viewed by anyone with SIPRNET access. It interfaces with a data repository and provides up-to-the minute updates on the location of vessels of interest. A user can drill down into specific areas in the view to get a closer view of what ships are out there. Once a particular ship is clicked on, it will send the user via a hyperlink to the details known about the vessel of interest. WEBTAS has an easy to use GUI and provides a plethora of information to a multitude of organizations. RBAC could potentially be applied to the WEBTAS data repository. The basic set up would be a Secret clearance and then different levels could be displayed on a multilevel security system ensuring those who meet whatever criteria (is required) would get access to the needed information.

F. RBAC ADVANTAGE

An important question to ask is: Why employ RBAC over other access control models? One reason is that RBAC only requires two mappings: roles to permissions and users to roles. It does not permit users to be directly associated with permissions. This solution can be much simpler to employ over access control lists (ACLs). While access control lists have been shown to be technically feasible to use, there are numerous disadvantages in using them:

- Difficult to manage data effectively
- ACL’s are bound to objects
- Unable to manage subject-based security policies

- End users do not own information to which they are allowed access
- An organization with a large number of users could become an administrative nightmare[22]

A large organization with many users, who each have permissions, requires a large number of user and permission associations. For instance, when a user switches positions within an organization, the switching requires a thorough review, addition, and deletion of user/permission associations of each server. In addition, there is an administrative cost:[23]

- U = set of individuals in a job position
- P = set of permissions required for that job position
- The number of associations required to directly relate the individuals to permissions = |U| x |P|

In Role-Based Access Control, this switching within a company is simplified into the formula |U| + |P| because the switch only requires two changes by an administrator:

- Remove user/role association for old job
- Insert user/role association for new job

The number of user/role and role permission associations required to authorize each user in set U for each of the permissions in the set P (P represents the role) = |U| + |P| which is < |U| x |P|. The summation of the sum of all users and permissions associated with the total number of job positions is less than the product of the summation of all users and permissions associated with the total number of job positions. The mathematical notation looks like this: [24]

---

[22] Chris Agar, Kevin Smith, and Troy Wright. *Role Based Access Control*. PowerPoint Presentation, April 18, 1998.

[23] Ibid.

[24] Ibid.

$$\sum_{i}^{n} {}^{jw}(|U_i| + |P_i|) < \sum_{i}^{n} {}^{jw}(|U_i| * |P_i|) \qquad \text{(Eq. 1)}$$

An example of the previously mentioned advantages of RBAC can be visualized with a generic example using two of the Maritime Intelligence Fusion Center Roles[25]:

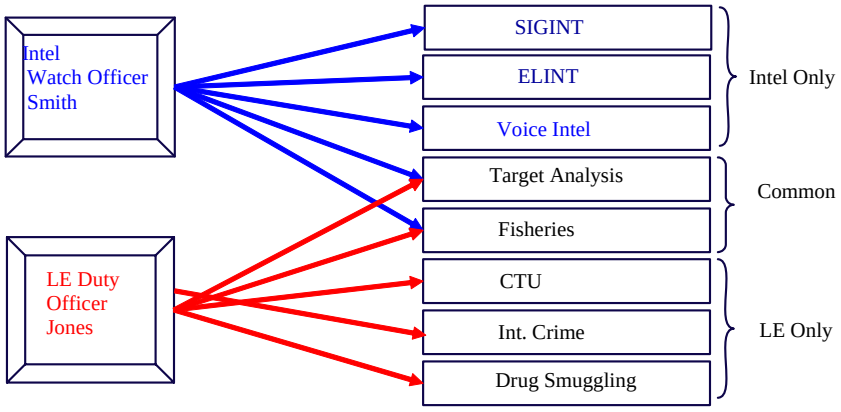

Figure 6. MIFC RBAC example one

For these two watch officers, the total number of associations is |2| X |5| = 10. If, for example, the IWO (Lt. Smith) becomes a LE Duty Officer, this would require the below deletions and additions:

[25] Chris Agar et al.

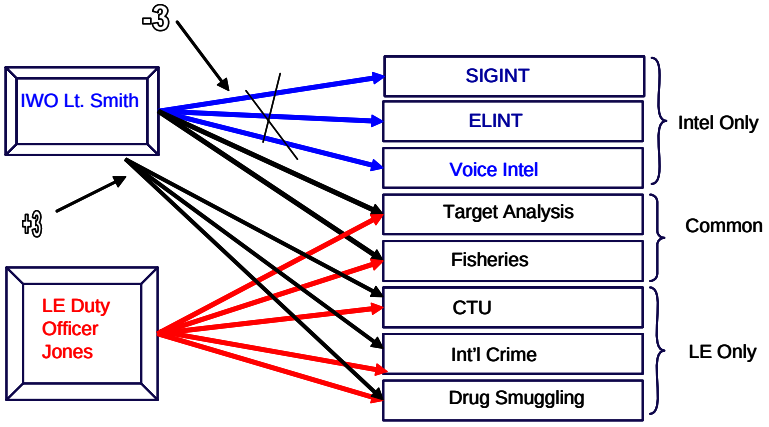

Figure 7. MIFC RBAC example two

In the case above, the top three blue associations are eliminated and three more are added to CTU, International Crime, and Drug Smuggling. This is represented by the '-3' for deletions and the '+3' for additions. Target Analysis and Fisheries were already common associations so they remain the same. The total amount of changes necessary is |-3| + |+3| = 6. Now, in the below diagram, we have inserted two roles, that of Intelligence Watch Officer and the other is the Law Enforcement Duty Officer.

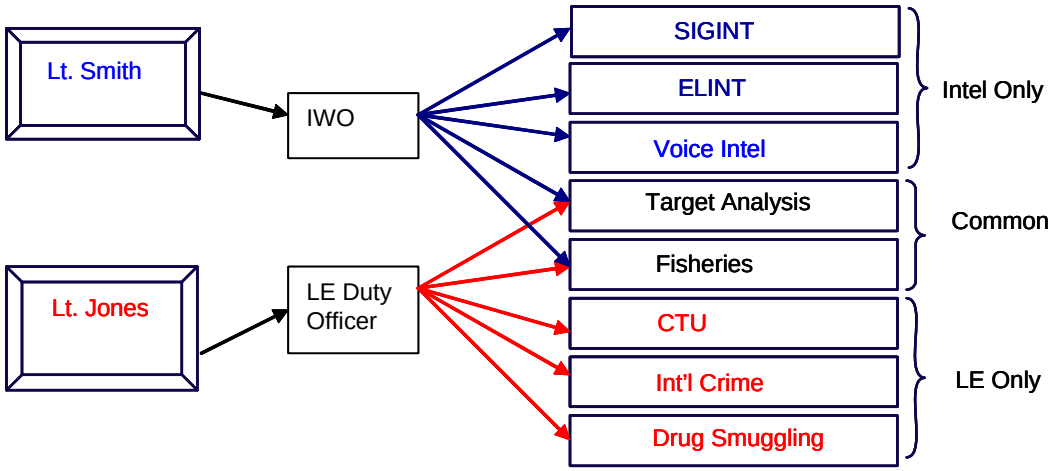

Figure 8. MIFC RBAC example three

Now, if Lt. Smith is to assume the role of LE Duty Officer as above, the administrator will only perform two additional associations(|-1| + |+1| = 2) instead of six, as shown in the following diagram.

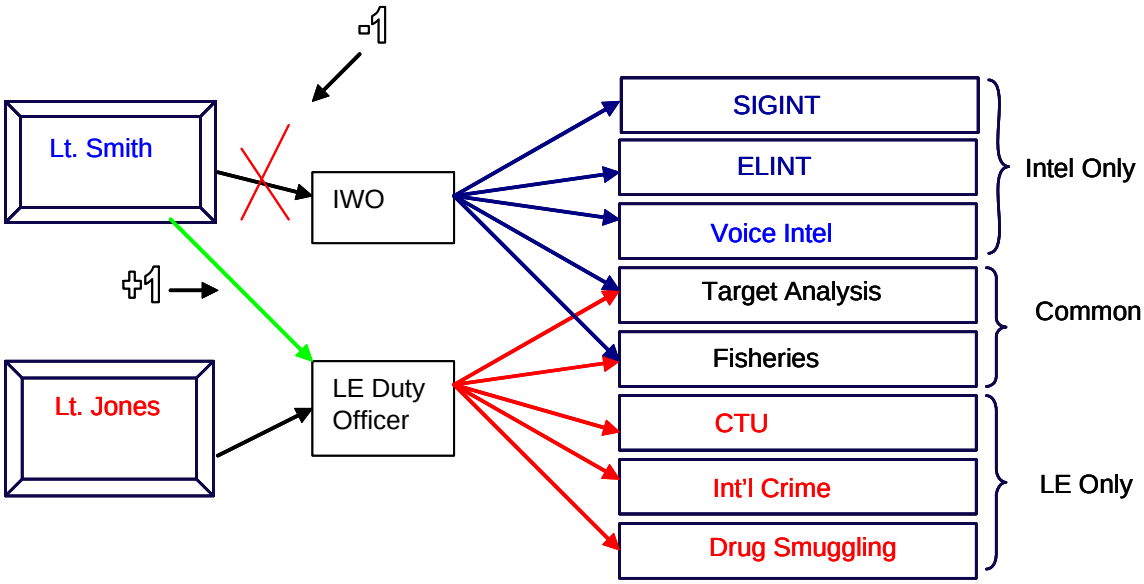

Figure 9. MIFC RBAC example four

The preceding examples illustrate how employing RBAC can simplify the specification, maintenance, and enforcement of access control policy. While employing RBAC, one may encounter an initial heavy start up costs as roles are assigned and users are mapped to them. However, once that initial mapping is complete, updating the access policy and mappings will be much less arduous a task than if the policy and mappings were to be maintained on a user-by-user basis.

G. RBAC AND MLS

Kuhn[26] describes how RBAC can be implemented without any major changes to Multi-Level Security (MLS) systems. Hierarchical RBAC can be applied and these roles are mapped to MLS labels. In this paper, RBAC is managed at a level that corresponds closely to the organization's structure. As usual, each user is assigned one or more roles and each role is assigned one or more privileges. The paper discusses how RBAC can be implemented using the controls available on lattice-based MLS systems. According to Kuhn's paper, the mapping of RBAC to MLS categories can be done in a few ways depending on the organization's needs. One way is to establish a mapping between RBAC privileges and pairs of MLS categories. If there are 64 categories within an MLS system, there will be 2016 privileges which could be mapped to MLS categories. The number of privileges *p* given *n* categories is computed as follows:

$$p = \frac{n^2 - n}{2} \qquad \text{(Eq. 2)}$$

Using combinations, the largest number that could distinguished, *d*, is $1.83 * 10^{17}$, that is,

$$d = \frac{n!}{\frac{n}{2}! * \frac{n}{2}!} \qquad \text{(Eq. 3)}$$

Of particular interest to the military is the potential application of RBAC to operate simultaneously with a MAC system. In a military system that supports both roles and MAC, if a system is labeled system low, the user can activate any process available to that role and apply that process to any data for which they are cleared by virtue of the MAC policy. In conclusion, the paper states that it is much easier to utilize RBAC as a

---

[26] D. Richard Kuhn. *Role Based Access Control on MLS Systems Without Kernel Changes.* Proceedings of the Third ACM Workshop on Role-based Access Control; (Fairfax, Virginia: ACM Press, 1998), 26**.**

single trusted process than to rely on MLS to control access to objects and modify the kernel of a secure system or build a system from the ground up.

As mentioned previously, two of the most commonly used methods for implementing access control are Discretionary Access Control and Mandatory Access Control. When examining MLS, a further discussion of these two policies is required. The key concept of MAC is that the user does not have discretion as to whether to abide by the policy. The system enforces the policy. This is the opposite of discretionary policy, in which the user chooses which policy to enforce. In terms of establishing multilevel security, we generally are talking about MAC. In general, the purpose of MAC is to prevent the unauthorized flow of data (and not much else). RBAC on the other hand is more flexible, and can support a variety of policies. It can be used, for example, to implement an information flow policy such as MAC, as well as an integrity focused policy.[27]

We already noted that a role can be seen as a set of permissions (privileges). To implement RBAC in a MLS system, there must be a trusted interface that brokers the assignment of accesses to resources by users, and that is controlled in accordance with the RBAC policy. The trusted interface must map roles and privileges to corresponding sets of categories, as shown below. When a user attempts to establish a session, the trusted interface verifies the user has approved access to the desired role.[28]

---

[27] D. Richard Kuhn. Role Based Access Control on MLS Systems Without Kernel Changes, 26.

[28] D. Ferraiolo, R. Kuhn, and R. Chandramouli. *Role-Based Access Control*. (London: Artech House, 2003), 130.

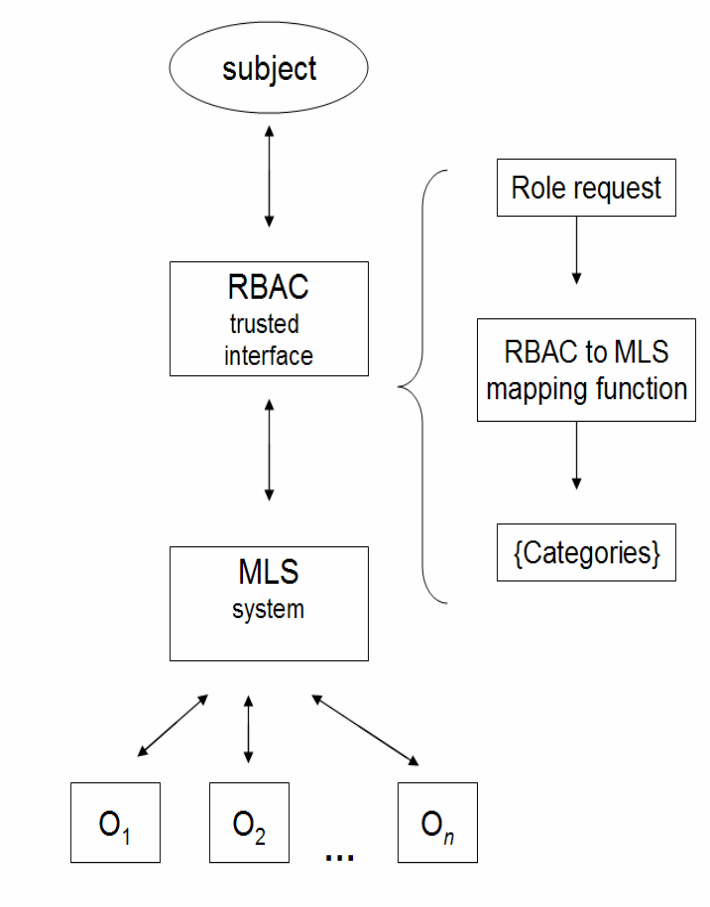

Figure 10. RBAC/MLS interface [29]

[29] D. Ferraiolo, R. Kuhn, and R. Chandramouli, 131.

THIS PAGE INTENTIONALLY LEFT BLANK

III. IMPLEMENTATION OF RBAC

A. USING AN RBAC MODEL SCENERIO #1

In this section we examine the flow of data and roles as they could pertain to an example related to us by members of the Maritime Intelligence Fusion Center (MIFC) located in Alameda, California. The scenario includes roles that are triggered as the situation warrants and the type of RBAC that will be initiated. The flow of data and roles is described in a flow chart in figure 11.

The United States Embassy in Hong Kong sends a facsimile to MIFC providing intelligence about a boat carrying immigrants who may be heading to the United States via Mexico or Central America. The intelligence reports that the ship will be heading towards Mexico where the migrants will disembark and then cross by land into the United States. The Hong Kong consulate does not regularly communicate with the MIFC. The role of 'consulate' is established to maintain communications and data flow between the two organizations. The facsimile is received by the MIFC 'watch officer', a role that is already pre-established. The watch officer is the linchpin in providing data to his or her superiors and initiating action. This is a common role and will already be activated by the watch officer as he or she comes on duty. The fax is then sent by the watch officer to the 'tactical analyst' for review. Again, this role is already enacted as he or she takes the watch. The intelligence is analyzed and sent back to the watch officer. The watch officer reports to the Command Duty Officer (CDO) and Commander. These roles will again already be established. Other important roles that are established include the 'legal' role and 'Foreign Affairs Officer' role to ensure the legality of an impending operation and to coordinate with other countries. In this case, a 'Mexican Law Enforcement' role needs to be established. This is an attribute of CBAC in which data is shared among organizations or countries that participate in a given operation. This role would be limited as the United States may not want to share all the data that it has, but just enough for the coalition partners to help the United States or other coalition partners to achieve an agreed-upon goal.

The data collected on the suspected illegal-immigration operation is shared according to the need-to-know attributable to each role-organization pair (e.g., Mexican Navy watch officer may not have a need to know the coordinates of the U.S. Navy ship that is tracking the vessel carrying the illegal aliens) for a specific time interval (e.g., the Mexican Navy watch officer would not have a need to know once the interdiction mission is over). The latter condition is an example of why Temporal Role-Based Access Control needs to be employed along with DRBAC and CRBAC. As the following diagram shows, some roles are revisited and new ones are created. New roles include the Immigration and Customs Enforcement (ICE) agent on the ground in Mexico and the Field Intelligence Support Team (FIST) which is an entity separate from the MIFC's chain of command. Once the data is shared and looped back to the 'watch officer,' he can bring in the 'vessel targeting and analysis team' to locate and track the vessel of interest. This will require the assistance of other organizations such as the U.S. Navy or a foreign Navy. The Navies in this example will need to have access to the common operating picture and this can be done via CBAC. These organizations do not need to know all the details of the operation, just enough to locate and track the target of interest. Finally, once all this occurs and the vessel is located, the Coast Guard can perform its boarding; the access rights to the data for those roles can then be changed to reflect the new situation.

Table 1. Role Definitions for Scenario #1

Role	Organization	Sub role	Description
Watch Officer	MIFC	IWO	Responsible for coordinating the actions and responses for MIFC based on intelligence reports and recommendations from his watch team. Makes judgment calls on intelligence reports to determine where the intel will need to be sent. Reports to the Command Duty Officer.
Watch Officer	MIFC	CDO	Oversees the IWO and the watch floor at MIFC and receives reports from the IWO. Will coordinate with the staff and Commander to determine courses of action.
Analyst	MIFC	SIGINT	Examines signals intelligence and makes recommendations to the watch officer.
Analyst	MIFC	ELINT	Examines electronic intelligence and makes recommendations to the watch officer. Coordinates intelligence gathering with various Field Intelligence Support Teams to develop/verify intelligence.
Analyst	MIFC	International Analyst	Determines if there is a threat, if it is credible and if it is plausible. Uses subject matter experts to further develop intelligence.
Analyst	MIFC	Vessel Targeting	Examines intelligence from various sources to formulate probable locations of the vessel of interest. Recommends search area to the IWO.
Analyst	MIFC	Counter-terrorism	Examines intelligence and determines if a terrorism threat exists. Checks watch lists for names and coordinates with other counter-terrorism agencies
Legal	MIFC	MIFC Legal Officer	Provides guidance to the MIFC Commander on any legal issues. Ensures all MIFC actions comply with federal and local laws and regulations.

Foreign Liaison	MIFC	Foreign Liaison Officer	Coordinates with the State Department and foreign governments in the prosecution of an active case that requires the assistance or involvement of a foreign government.
Foreign Country	Mexico	Navy/Law Enforcement	Any branch of the Mexican government that plays a role in the apprehension or prosecution of the suspected illegal immigrants.
Interdiction	US Navy	Various commands at sea or ashore	Executes or provides assistance in the apprehension of target vessels at sea.
Interdiction	USCG	Various commands at sea or ashore	Executes or provides assistance in the apprehension of target vessels at sea.
Interdiction	USCG	Immigration Customs Enforcement Team	Responsible for developing and gathering intelligence on illegal immigration into the United States. Work with federal and local law enforcement in the prevention and apprehension of illegal immigration.
General Intel	Any	Hong Kong Embassy	Provides unsolicited and unverified intelligence to MIFC. With the General Intel Role, there is no pre established relationship and this role can be activated for unsolicited intelligence such as this scenario.

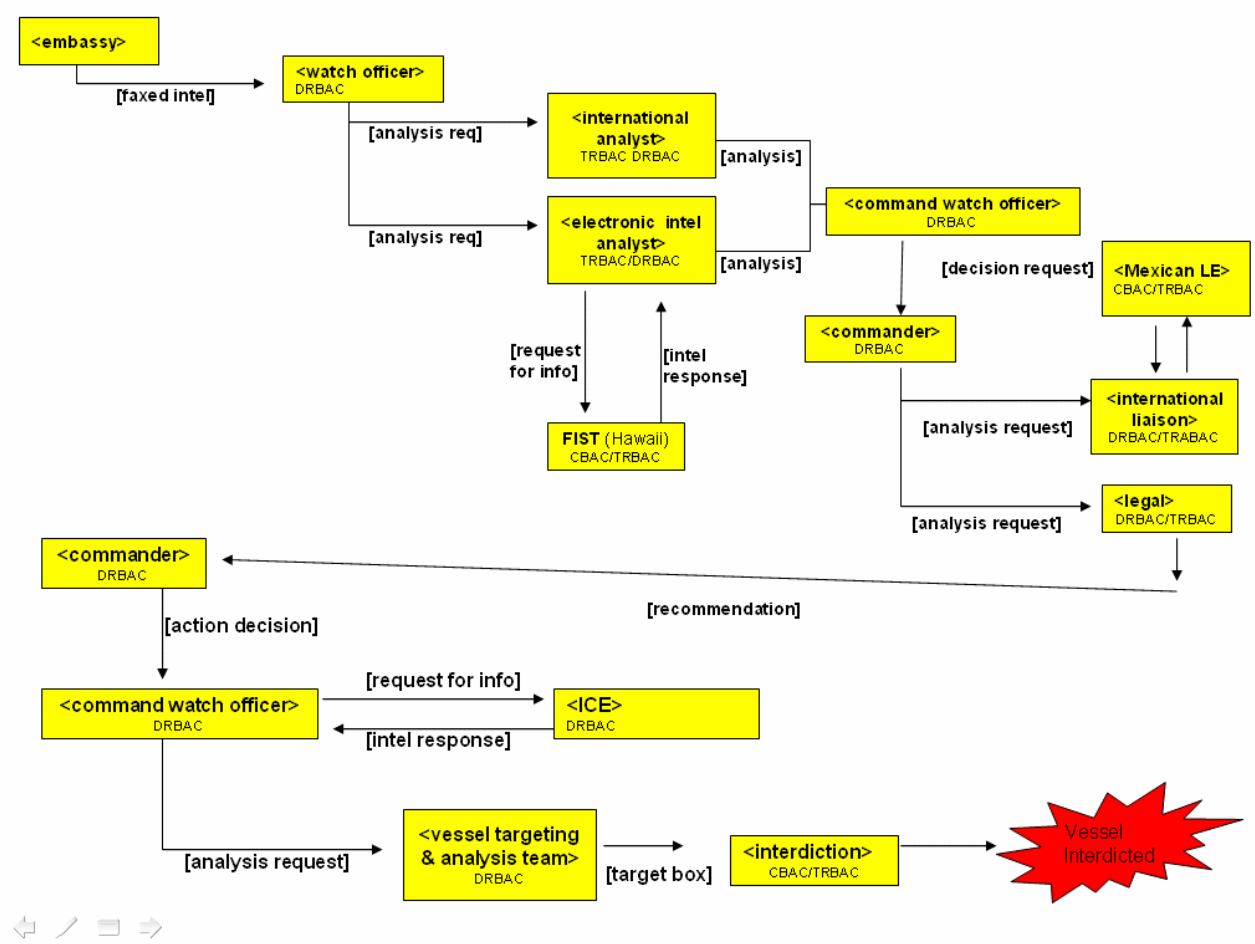

Figure 11. Scenario #1

B. SCENARIO #1 WITH INFORMATION BROKER AND REPOSITORY

In this updated version of our scenario, we have introduced the idea of the Information Broker and information repository. This improvement upon our previous example allows streamlined access for the users of the repository and the providers to the repository. For example, in the first occurrence of the Information Broker, the watch officer at MIFC sends his intelligence to the Information Broker and is a provider of data. The watch officer requests an analysis of the data from his team of analysts who then

retrieve the data from the repository via the Information Broker. The team of analysts conducts its analysis and reports the results of the analysis to the repository where the watch officer can retrieve the analyzed intelligence. This may be a simple example of the use of an Information Broker, but as the size and complexity of the mission increases, there may be a corresponding increase in the number of types and instances of roles (e.g., with the inclusion of roles played by Mexican law enforcement and military personnel). The Information Broker in our model stores, filters, and retrieves intelligence reports in the information repositories.

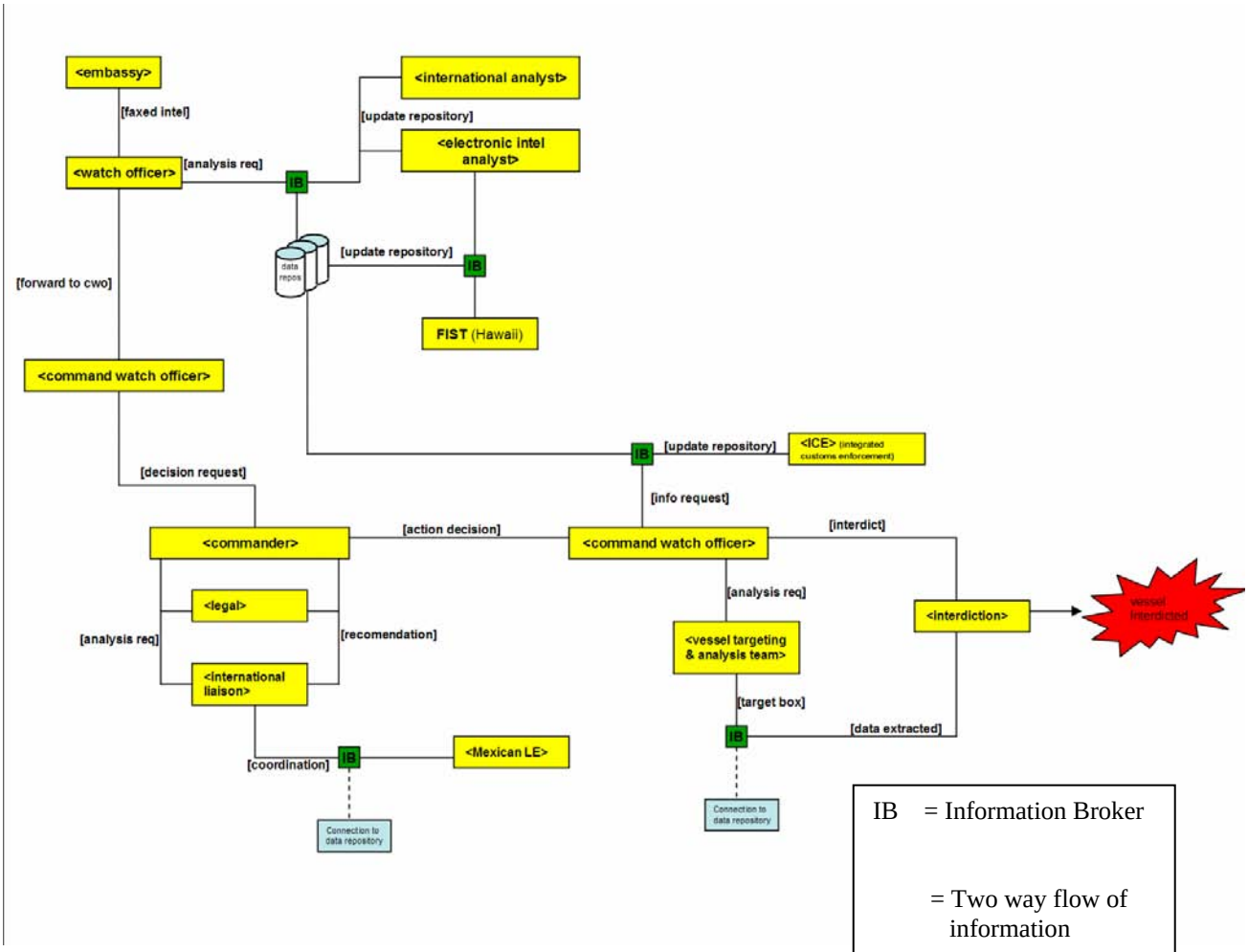

Figure 12. Scenario #1 with Information Broker

C. IMPLEMENTING AN RBAC MODEL SCENARIO #2

In this section we examine the flow of data and roles as they pertain to a fictitious, but potentially realistic situation. The flow of data and roles are described in a flow chart on the next page.

A foreign intelligence organization from the United Arab Emirates notifies the CIA that there is the possibility that a merchant vessel left Port Zayed two days ago with a concealed missile pod in one of its cargo containers. The missile pod can be exposed and be immediately used to target assets ashore and cause immense damage before law enforcement or military units can be mobilized to intercept the vessel or the threat missile. It is bound for the Port of Oakland (located in California) and is expected to arrive in two weeks. It's manifest and planned movement has been 'lost' or is not available. The ship is registered in the U.A.E and is named *Sandstorm*. It must be located and searched. The roles of 'foreign government' with numerous sub roles must be established. The intelligence is first received from a U.A.E. intelligence agency. Roles within the agency are added to the model so that RBAC policy can be specified regarding those roles. Since the United States does not want to share all data, it will be on a limited basis and Coalition Based Access Control (CBAC) will be utilized. As the situation progresses, other entities that become involved include 'NGOs' with roles that might include the captain of a civilian merchant vessel. U.S. and allied Navies are also activated to assist in locating and tracking the vessel of interest. Entities such as Foreign Allied governments could have roles that are also activated. Coordination is achieved via The U.S. State Department. As the ship proceeds, it is spotted by a US Navy P-3 aircraft flying surveillance over the Eastern Pacific Ocean. The P-3 reports its location and name, which is in turn entered into the MDA data repository where it triggers a flag to notify the Coast Guard that the *Sandstorm* has been located.

As this example progresses, entities such as U.S. Northern Command (NORTHCOM) will have activated roles such as 'Commander' or 'Watch Officer' because of the potential threat to the security of the United States. U.S. Pacific Command (PACOM), FBI and local law enforcement are all entities from the Oakland area which

would have activated roles in this situation. Before the ship comes too close to the shore to launch its missiles, it is approached and stopped by a US Navy Destroyer with a Coast Guard Law Enforcement Detachment aboard. The information regarding the *Sandstorm* was accessed aboard the destroyer by the Tactical Action Officer with the role of Watch Officer. As the ship is boarded by the Coast Guard team, the Captain of the port in Oakland is receiving reports from a Sea Marshall and boarding team on the deck of the *Sandstorm*. The roles of Sea Marshall and port Captain are pre-established and are activated once they become involved in the interdiction process.

Finally, after searching the vessel, the missile pod is discovered and arrests are made. This is where the law enforcement agencies are included and CBAC is again used. Throughout the whole process, TRBAC is used to specify the activation and deactivation of roles.

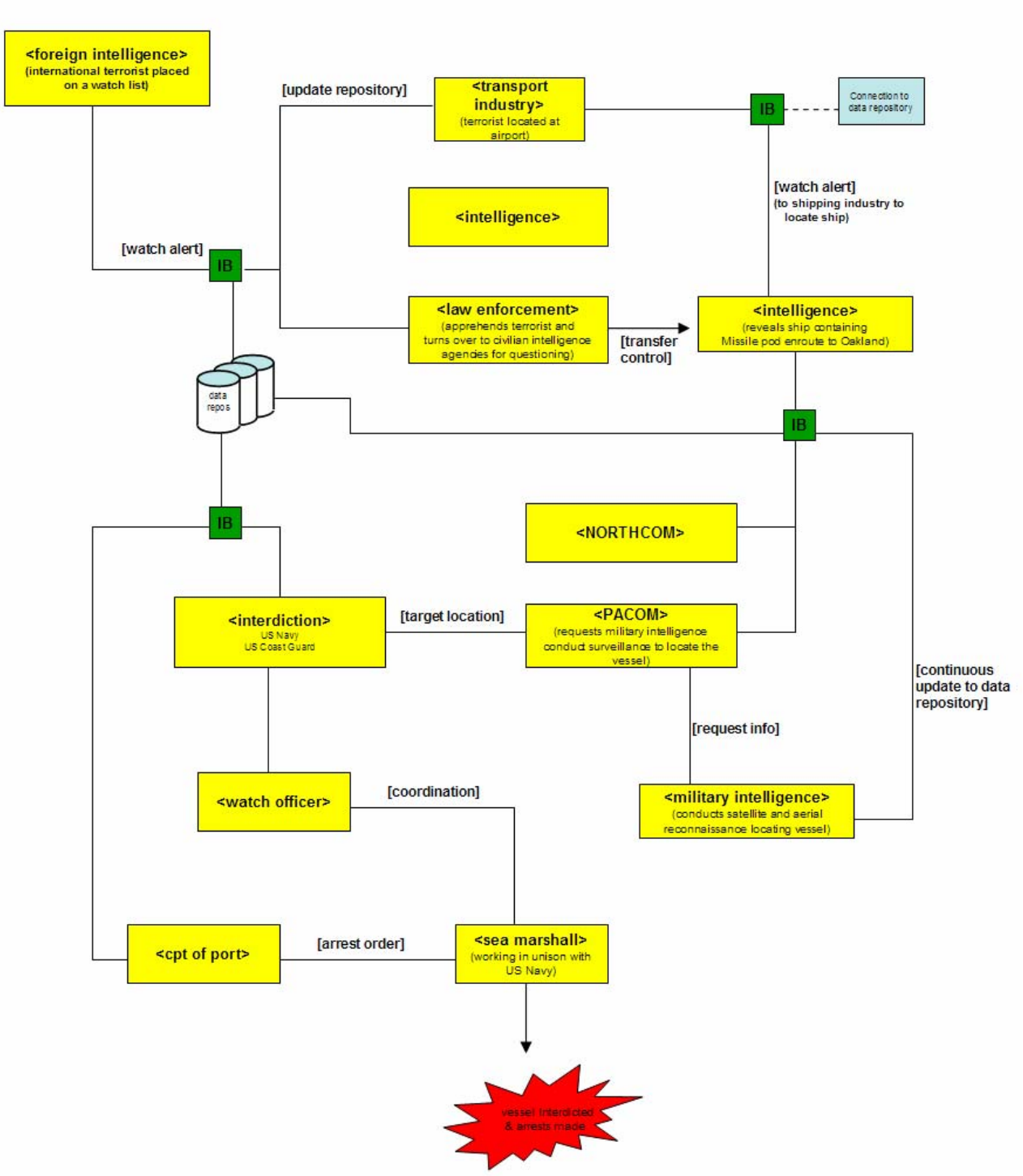

Figure 13. Implementing RBAC example

D. REASONS FOR COALTION RBAC

In this paper, the term coalition is used extensively. Our definition of a coalition is an alliance (permanent or temporary) formed to achieve a common goal within the context of MDA/MDP. It can be between organizations within the same country or transcend borders into allied countries. Within a coalition, there are relationships among roles that are relatively invariant, for example, the relationship between a watch officer of the US Navy and his or her counterpart in the Mexican Navy. Situations can arise in which roles from different organizations need to be added or modified (i.e., the membership in the coalition in terms of roles can expand or contract) in order for the coalition to achieve its mission; the additions or modifications may be permanent or temporary in nature.

In our model, an information repository is a store of data and relationships between data controlled by an Information Broker. There are users of the information repository and providers of data to the repository. The Information Broker is the interface between the users and providers of data to the information repository. The levels of trust are determined on a case by case basis and the levels of details provided to the users of the data is determined by the Information Broker and distributed via the information repository. An example of a hierarchy of levels of trust is shown below.

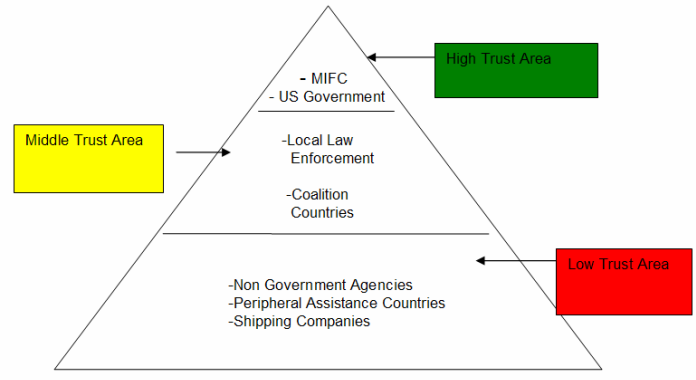

Figure 14. Trust triangle for CBAC

E. CORE AND AD-HOC COALITIONS

Without coalitions, there would be no need for DRBAC or CBAC. All the modeling could be done using the RBAC model without any extensions to represent group membership. Coalitions formed within MDA can be permanent or ad hoc. Membership in coalitions can be permanent or temporary; we refer to the former as core members and the latter as transient members. Members of an ad hoc coalition can be created on the fly and are used as events warrant. It is impossible to create core coalition members for every possible scenario. Therefore, there must be methods in place that will allow for creating transient members and temporary coalitions on the fly. An issue here is who is responsible for creating and maintaining these roles. In our model, we leave the "who" up to the conveners of the coalition, but require that the addition and maintenance of roles be performed by the Information Broker. Ownership of an Information Broker does not imply authorization to set or change access control policies or add or remove members of the coalition. The owner of the IB is concerned only with accessing the data located within their repository and enforcing access control policies.

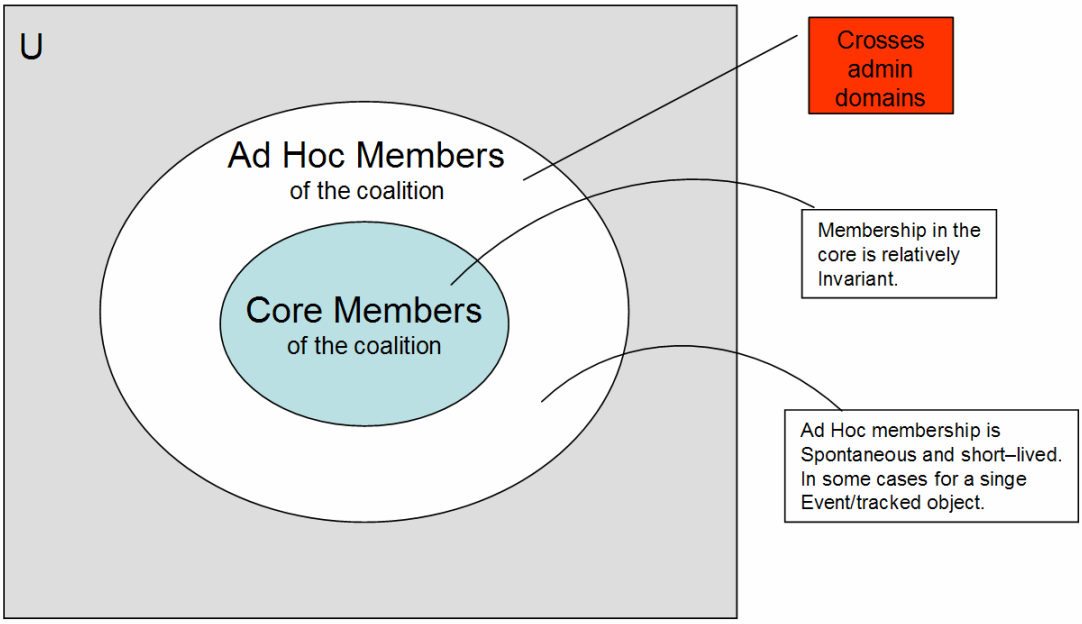

Figure 15. Coalition members

THIS PAGE INTENTIONALLY LEFT BLANK

IV. ASSESSMENT

A. DISTRIBUTED RBAC MODEL FOR SCENARIO #1

The purpose of this section is to demonstrate a systematic formal approach showing that Role-Based Access Control can be done, explain how it can be done, and most importantly explaining why it is appropriate for Maritime Domain Awareness. The proof uses the model proposed by Freudenthal et al and will be used as a base for our example.[30] Existing roles will change and new roles will be defined and there will be relationships created between existing role and new roles created outside the organization. Our first example will follow scenario #1 presented in the previous section. In this example, LT Smith and LT Rivera are fictional characters for fulfilling specific roles, MIFC is the Maritime Intelligence Fusion Center, and the modeling example provided is a small sample space of the roles and organizations involved. The model itself is very dynamic and changes as needs require.

Entities: A public key that represents a principal or a resource, and defines a namespace that can contain roles. This namespace encompasses the entire range of possible players.

Form: cryptographic public key and a human-readable name

Examples: LT Smith; MIFC

Roles: A name within an Entity's namespace.

Form: Entity.LocalName

Example: MIFC.member

Role Delegations: Signed Certificates that extend access rights on some object to a subject. Access to an object by a subject can be extended by the issuer of the certificate.

Form: [Subject → Object] Issuer

[30] Eric Freudenthal, T. Pesin et al., 411-420.

An Object is a Role, an Issuer is an Entity, and a Subject is a Role or an Entity. Therefore, the issuer of the access rights, in our example the controller of the data repository, extends access rights of an object in the data repository to a subject.

Example: [MIFC IWO → MDA Data repository] MIFC

Distributed RBAC includes three major types of delegations:

(1) Self-certified Delegation: An Issuer A grants role A.a to some Subject. The role granted is defined within A's namespace.

Form: [Subject → A.a] A

Example: [LT Smith → MIFC.watchOfficer] MIFC

LT Smith is granted all permissions of the role MIFC.watchOfficer.

(2) Assignment Delegation: Entity B grants some Subject the right to delegate Role A.a to others. The tick (') indicates that the Subject can further delegate the Role.

Form: [Subject → A.a'] B

Example: [MIFC.watchOfficer → MIFC.member'] MIFC

This effectively allows an entity that possesses permissions to delegate the role MIFC.member' to others as well.

(3)Third-Party Delegation: In third-party delegation, some Issuer B exercises their right to delegate a Role defined in A's namespace. In this case, A and B are not the same entity. In (2), that may or may not be the case.

Form: [Subject → A.a]B

Example: [LT Rivera → MIFC.member] MIFC

In essence, LT Rivera can be granted all the permissions associated with MIFC.member. This is granted through the MIFC server which can control access to the MDA data repository to a coalition member.

Valued Attributes: A name within an Entity's namespace, disjoint from the role namespace that can be set to a numeric value in order to modulate access level is a valued attribute. Zero or more Valued Attributes can be set in conjunction with the delegation of a Role.

Form: [Subject → Object with A.Attribute1 <*Operator*>=<Value> <and B.Attribute2 <*Operator*>=<Value>>*] C

A, B, and C can either be the same entity, or different entities, or any combination thereof. The "with" clause specifies the first Valued Attribute in the delegation; subsequent attributes are specified using "and" clauses.

Example: [Mexico.member → MIFC.member with MIFC.shipDes <= S and MIFC.ShipCar <= S] MIFC

In this example a Mexico member is allocated all the permissions associated with a MIFC member except (for whatever reason) that the Mexico member can only read details of the target ships location within 10 miles and details of the ships cargo classified at or below the Secret (S) level.

Delegation of Assignment for Valued Attributes: These delegations give the Subject the right to set the Object Attribute in future delegations written by the Subject. While the Valued Attribute is not a Role, the right to set it is a Role, and therefore can be the Object of delegations.

Form: [Subject → Entity.Attribute <operator>='] Issuer

Example: [MIFC.vesselTracking → Mexico.vesselTracking -= '] MIFC

In the above case, vesselTracking is given the right to modify the Mexico.vesselTracking access rights within a set limit.

Credential Management: These delegation annotations provide mechanisms to discover credential chains and control credential lifetime.

Discovery Tags Form: [Subject<Discovery Tag> → Object<Discovery Tag>] Issuer

<acting as Role, Discovery Tag>

Expiration Date: A date after which the delegation is no longer valid.

Form: [Subject → Object <expiry: date>]

Example: [Mexico.member → MDA.data repository <expiry 10/10/05>]

This is used as a tool for tracking expiration dates of roles and access privileges.

The information below describes the delegations supporting LT Rivera of Mexico's access to MIFC resources.

(1) [LT Rivera → Mexico.member] Mexico

(2) [Mexico.member → MIFC.member

with MIFC.shipDes <= S

and MIFC.shipCargo <= S] LT Smith, MIFC

(3) [LT Smith, USCG → MIFC.account] MIFC

(4) [MIFC.account → MIFC.member'

with MIFC.shipDes <= '

and MIFC.shipCargo <='] MIFC

(5) [MIFC.member → MIFC.access

with MIFC.shipDes <= TS

and MIFC.shipCargo <= TS] MIFC

Table 2. Delegation of LT Rivera's Access

In Table 2, a full implementation of DRBAC including detection, authorization and monitoring is modeled. Mexican Intelligence Agent LT Rivera is able to take advantage of a coalition between Mexico and MIFC to obtain data through MIFC. Delegation step (1) identifies LT Rivera as a Mexico.member. Delegation step (2) defines

the coalition between Mexico and MIFC as established by LT Smith. Step (2) also provides limitations or restrictions as specified by MIFC delegate LT Smith. These limitations can be set, removed, or modified on a case by case basis depending on the strength or desired strength of the coalition. LT Smith is authorized to provide this delegation as described in delegation steps (3) – (5).

The below diagrams are a distributed proof construction of the initialization and final steps in the DRBAC process. This case study starts off with LT Rivera establishing a connection to a MIFC server to access information (step 1). In this case the foreign coalition role of 'Mexico' authenticates itself to MIFC using public-key cryptographic protocol and requests access to the data on LT Rivera's behalf by passing on delegation (1) which validates LT Rivera as a Mexico.member. To authorize access, the MIFC server must find a proof for Mexico.member ⇨ MIFC.access. When combined with delegation (1) proves that LT Rivera is authorized access to applicable MIFC data (LT Rivera ⇨ MIFC.access).

The MIFC server queries its trusted local wallet for the required proofs as seen in step 2. If it fails to find it locally, the wallet attempts to discover the delegations necessary to build the proof. The wallet will contact the home wallet corresponding to the role Mexico.member and issue a query and discovers that there is a defined relationship between the roles Mexico.member and MIFC.member. The server wallet now has a chain from LT Rivera to MIFC.member. There is still an outstanding requirement that would authorize MIFC members to MIFC data (MIFC.member ⇨ MIFC.access). A direct query is issued for a subject to object search involving MIFC.member ⇨ MIFC.access (step 4).

The results of this query are a self certified delegation. We now have proof showing LT Rivera has access to MIFC data (LT Rivera ⇨ MIFC.access).

> Delegations from this proof are inserted into the local wallet, which is trusted to verify signatures and establish its own validation subscriptions (step5).[31]

[31]Eric Freudenthal, T. Pesin et al, 419.

At this point, limitations and restrictions can be placed on access to data. In our example, we arbitrarily assigned the ship's ultimate destination and cargo as limiting factors. Therefore, access to this information could be restricted to Mexican coalition members at the Secret level and below.

In step 6, the proof is returned to the original requester and stored as an object. This object allows for the continuous monitoring of delegations authorizing LT Rivera's access. This continuous monitoring could implements the temporal aspects of RBAC, providing limited access to data based on time.

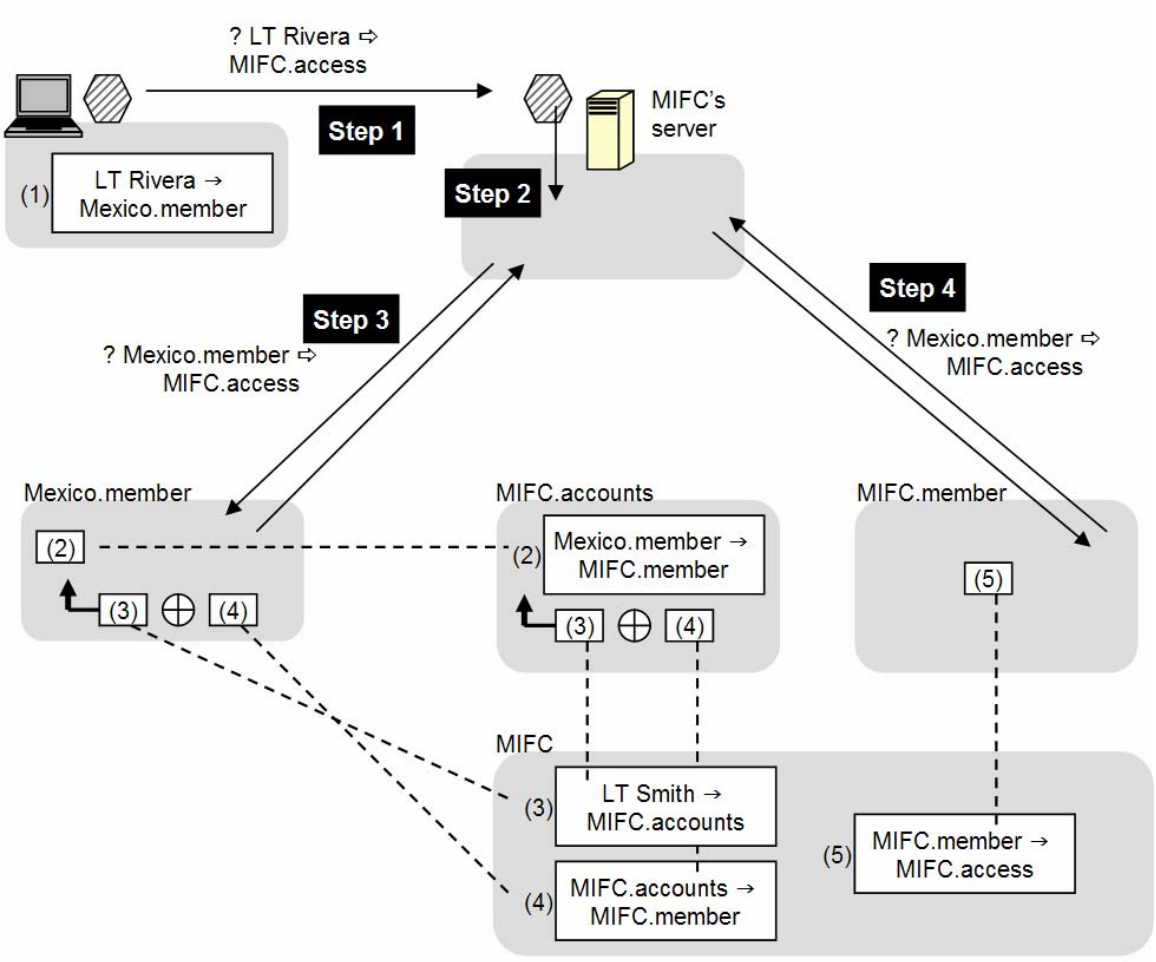

Figure 16. MIFC and Mexico Proof Diagram Initialization

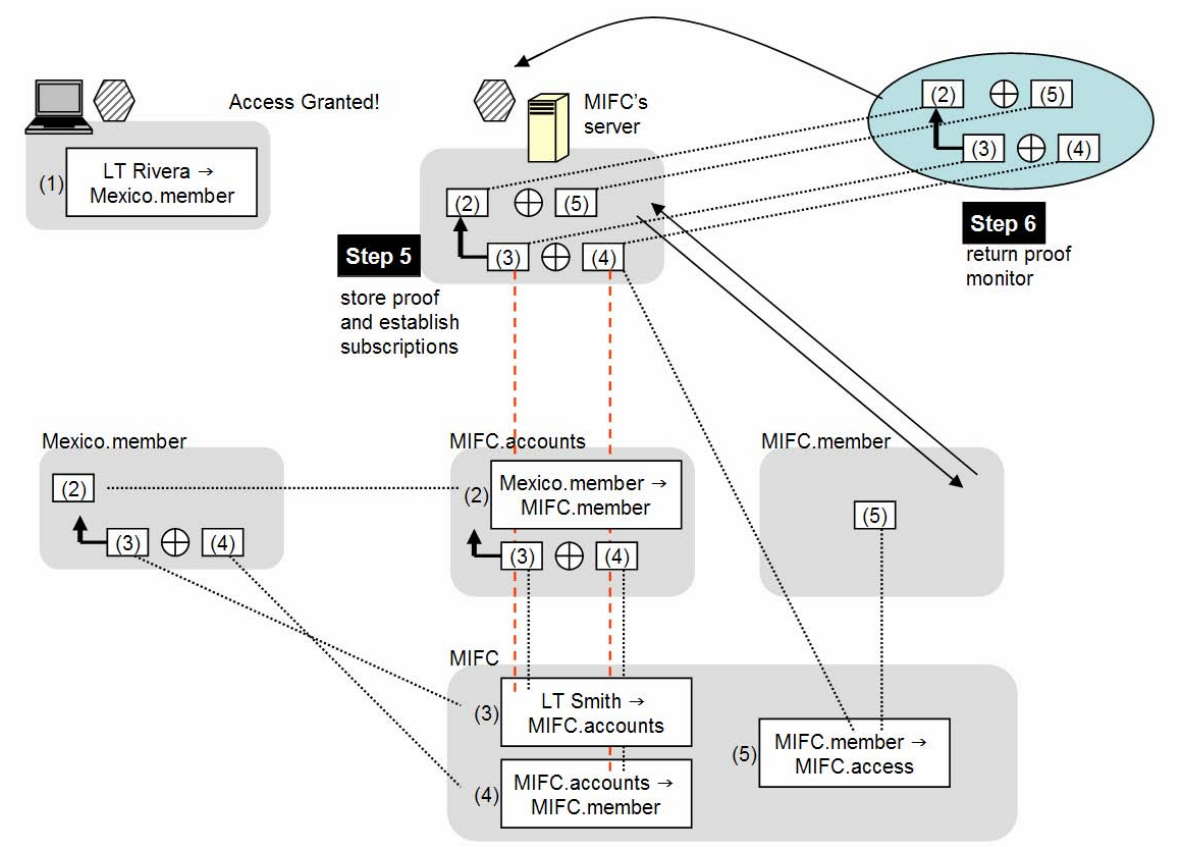

Figure 17. MIFC Proof Diagram Complete

B. DISTRIBUTED RBAC MODEL FOR SCENARIO #2

The purpose of this section is also to demonstrate a systematic formal approach showing that Role-Based Access Control can be done. This proof will be based on scenario #2 in which a missile pod is concealed on a tanker ship and is bound for the Port of Oakland. This proof also uses the model proposed by Freudenthal et al and will be used as a base for our example.[32] In this example, every role and player will not be modeled and only a small subset of them will be used. Specifically, LT Smith is again a fictional character at MIFC and CDR Thomas is a fictional character at United States

[32] Eric Freudenthal, T. Pesin et al., 411-420.

Northern Command. Even though this scenario does include foreign roles, those roles will not be included in this proof.

Entities: A public key that represents a principal or a resource, and defines a namespace that can contain roles. This namespace encompasses the entire range of possible players.

Form: cryptographic public key and a human-readable name

Examples: LT Smith; MIFC

Roles: A name within an Entity's namespace.

Form: Entity.LocalName

Example: MIFC.member

Role Delegations: Signed Certificates that extend access rights on some object to a subject. Access to an object by a subject can be extended by the issuer of the certificate.

Form: [Subject → Object] Issuer

Object is a Role, Issuer is an Entity, and Subject is a Role or an Entity. Therefore, the issuer of the access rights, in our example the controller of the data repository extends access rights of an object in the data repository to a subject.

Example: [MIFC IWO → MDA Data repository] MIFC

Distributed RBAC includes three major types of delegations:

(1) Self-certified Delegation: An Issuer A grants role A.a to some Subject. The role granted is defined within A's namespace.

Form: [Subject → A.a] A

Example: [LT Smith → MIFC.watchOfficer] MIFC

LT Smith is granted all permissions of the role MIFC.watchOfficer.

(2) Assignment Delegation: Entity B grants some Subject the right to delegate Role A.a to others. The tick (') indicates that the Subject can further delegate the Role.

Form: [Subject → A.a'] B

Example: [MIFC.watchOfficer → MIFC.member'] MIFC

This effectively allows an entity that possesses permissions to delegate the role MIFC.member' to others as well.

(3)Third-Party Delegation: In third-party delegation, some Issuer B exercises their right to delegate a Role defined in A's namespace. In this case, A and B are not the same entity. In (2), that may or may not be the case.

Form: [Subject → A.a]B

Example: [CDR Thomas → NORTHCOM.watchOfficer] MIFC

In essence, CDR Thomas can be granted all the permissions associated with MIFC.member. This is granted through the MIFC server which can control access to the MDA data repository to a coalition member.

Valued Attributes: A name within an Entity's namespace, disjoint from the role namespace that can be set to a numeric value in order to modulate access level is a valued attribute. Zero or more Valued Attributes can be set in conjunction with the delegation of a Role.

Form: [Subject → Object with A.Attribute1 <*Operator*>=<Value> <and B.Attribute2 <*Operator*>=<Value>>*] C

A, B, and C can either be the same entity, or different entities, or any combination thereof. The "with" clause specifies the first Valued Attribute in the delegation; subsequent attributes are specified using "and" clauses.

Example: [NORTHCOM.watchOfficer → MIFC.member with MIFC.shipDes = MIFC.watchOfficer and MIFC.ShipCar = MIFC.watchOfficer] MIFC

In this example the NORTHCOM watch officer is allocated all the permissions associated with a MIFC member including the data and information pertaining to the ship's destination and cargo equal to that of a MIFC watch officer.

Delegation of Assignment for Valued Attributes: These delegations give the Subject the right to set the Object Attribute in future delegations written by the Subject. While the Valued Attribute is not a Role, the right to set it is a Role, and therefore can be the Object of delegations.

Form: [Subject → Entity.Attribute <operator>='] Issuer

Example:[MIFC.vesselTracking → NORTHCOM.vesselTracking -= '] MIFC

In the above case, vesselTracking is given the right to modify the NORTHCOM vesselTracking access rights within a set limit, assuming NORTHCOM is tracking the vessel and aware of its progress.

Credential Management: These delegation annotations provide mechanisms to discover credential chains and control credential lifetime.

Discovery Tags Form: [Subject<Discovery Tag> → Object<Discovery Tag>] Issuer

<acting as Role, Discovery Tag>

Expiration Date: A date after which the delegation is no longer valid.

Form: [Subject → Object <expiry: date>]

Example: [MIFC.member → MDA.data repository <expiry 10/10/05>]

This is used as a tool for tracking expiration dates of roles and access privileges.

The information below describes the delegations supporting CDR Thomas of NORTHCOM's access to MIFC resources.

(1) [CDR Thomas → NORTHCOM.watchOfficer] NORTHCOM

(2) [NORTHCOM.watchOfficer → MIFC.member

with MIFC.shipDes = MIFC.watchOfficer

and MIFC.shipCargo = MIFC.watchOfficer] LT Smith, MIFC

(3) [LT Smith, USCG → MIFC.account] MIFC

(4) [MIFC.account → MIFC.member'

with MIFC.shipDes <= '

and MIFC.shipCargo <='] MIFC

(5) [MIFC.member → MIFC.access

with MIFC.shipDes <= TS

and MIFC.shipCargo <= TS] MIFC

Table 3. Delegation of CDR Thomas's Access

In Table 3, a full implementation of DRBAC including detection, authorization and monitoring is modeled. NORTHCOM watch officer CDR Thomas is able to take advantage of a coalition between NORTHCOM and MIFC to obtain data through MIFC. Delegation step (1) identifies CDR Thomas as a NORTHCOM.watchOfficer. Delegation step (2) defines the coalition between NORTHCOM and MIFC as established by LT Smith. Step (2) also provides limitations or restrictions as specified by MIFC delegate LT Smith. These limitations can be set, removed, or modified on a case by case basis depending on the strength or desired strength of the coalition. In this case, CDR Thomas is authorized to view all the data that a MIFC watch officer is entitled to see. This relationship is stronger than the previous scenario because the coalition between MIFC

and NORTHCOM is more trustworthy than the coalition between MIFC and Mexico. LT Smith is authorized to provide this delegation of permissions as described in delegation steps (3) – (5).

The below diagrams are a distributed proof construction of the initialization and final steps in the DRBAC process. This case study starts off with CDR Thomas establishing a connection to a MIFC server to access information (step 1). In this case the coalition role of 'NORTHCOM' authenticates itself to MIFC using public-key cryptographic protocol and requests access to the data on CDR Thomas's behalf by passing on delegation (1) which validates CDR Thomas as a NORTHCOM.watchOfficer. To authorize access, the MIFC server must find a proof for NORTHCOM.watchOfficer ⇨ MIFC.access. When combined with delegation (1) proves that CDR Thomas is authorized access to applicable MIFC data (CDR Thomas ⇨ MIFC.access).

The MIFC server queries its trusted local wallet for the required proofs as seen in step 2. If it fails to find it locally, the wallet attempts to discover the delegations necessary to build the proof. The wallet will contact the home wallet corresponding to the role NORTHCOM.watchOfficer and issue a query and discovers that there is a defined relationship between the roles NORTHCOM.watchOfficer and MIFC.member. The server wallet now has a chain from CDR Thomas to MIFC.member. There is still an outstanding requirement that would authorize MIFC members to MIFC data (MIFC.member ⇨ MIFC.access). A direct query is issued for a subject to object search involving MIFC.member ⇨ MIFC.access (step 4).

The results of this query are a self certified delegation. We now have proof showing CDR Thomas has access to MIFC data (CDR Thomas ⇨ MIFC.access). "Delegations from this proof are inserted into the local wallet, which is trusted to verify signatures and establish its own validation subscriptions (step 5)."[33] At this point, limitations and restrictions can be place on access to data. In our example, we arbitrarily assigned the ship's ultimate destination and cargo as controlling factors. These factors

[33]Eric Freudenthal, T. Pesin et al., 419.

could either be limiting or non-limiting. In this case the factors of ship's cargo and destination are non-limiting as access is granted to CDR Thomas up to the MIFC watch officer level.

In step 6, the proof is returned to the original requester and stored as an object. This object allows for the continuous monitoring of delegations authorizing CDR Thomas's access. This continuous monitoring could implements the temporal aspects of RBAC, providing limited access to data based on time.

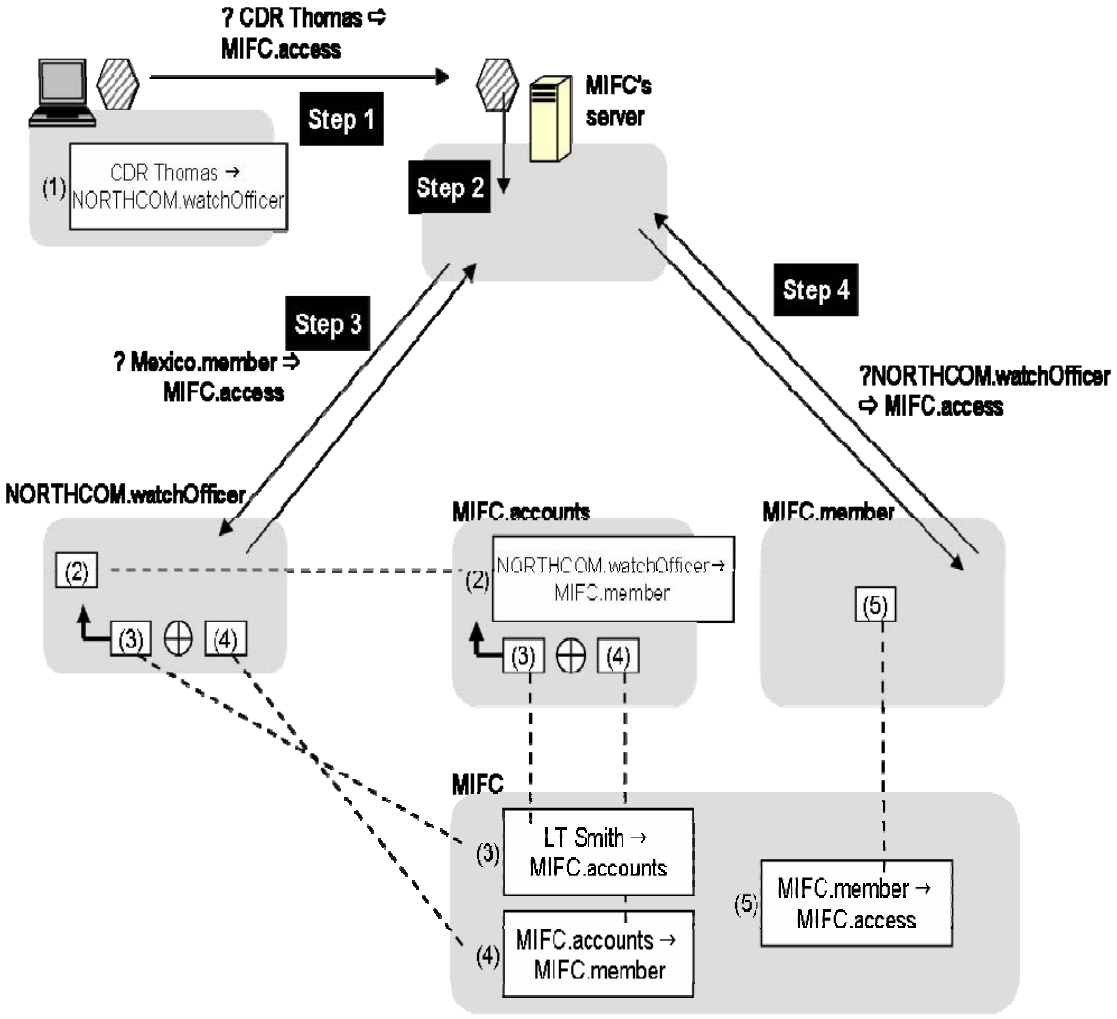

Figure 18. MIFC and NORTHCOM Proof Diagram Initialization

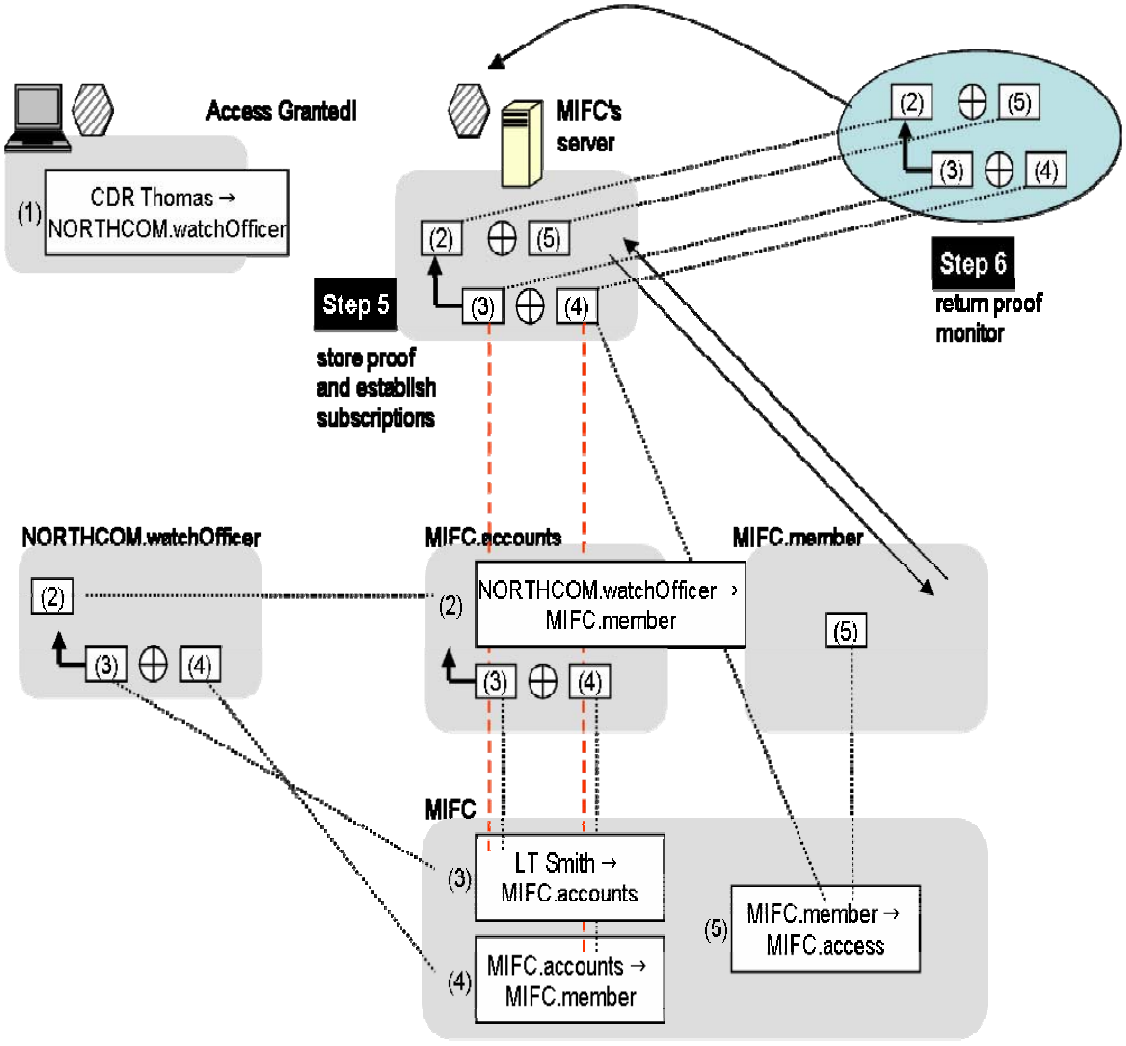

Figure 19. MIFC and NORTHCOM Proof Diagram Complete

C. GENERIC TEMPORAL RBAC MODEL

Temporal RBAC is another extension of the basic RBAC model. As described in section II, part C of this thesis, the features of TRBAC that are important to our modeling are that it supports periodic activation and deactivation of roles and the potential of specifying temporal dependencies among the activations or deactivations of roles by using role triggers. The ideas for modeling this aspect of RBAC are taken from Elisa

Bertino et al and their paper on Temporal Role Based Access Control.[34] The model below is a generic model that is not derived from any specific example, but does use MIFC as a base. First, a few definitions must be clarified before commencing the model:

(1) Event Expressions: have the form *activate R* or *deactivate R* where R ϵ Roles.

(2) Prioritized Event Expressions: have the form *p:E* where *p* ϵ Periodic Expressions that denote an infinite set of time instants and E is an event expression or the occurrence of some event.

(3) Role Status Expressions: have the form *active R* or *inactive R,* where R ϵ Roles.

(4) Role Activation Base: a set of elements that include periodic events *I* (time interval), *P* (periodic expression), and *p:E* (a prioritized event expression). It will also include role triggers that have a simple event expression E, role status expression C, prioritized event expression p:E, all over a certain change in time Δt. Additionally, the events described in the below example have priorities attached to them. The relationship is VH > H > M > L where VH is Very High, H is High, M is Medium and L is Low priority. The time to start and finish the role activations is indicated within the [ ]. The start date and time is first followed by the end time.

The below figure is an example that shows role activations and triggers over time using the symbols defined above and a simple arbitrary example of the watch rotation at MIFC. This is a simplified example where there are only two watches, which would most likely not be the case.

(PE1) [1/1/2005:0000, ∞] (Night-time → activate mid-watch IWO) VH

(PE2) [1/1/2005:0000, ∞] (Day-time → deactivate mid-watch IWO) VH

(PE3) [1/1/2005:0000, ∞] (Day-time → activate day watch IWO) VH

(PE4) [1/1/2005:0000, ∞] (Night-time → deactivate day watch IWO) VH

(RT1) (Activate night watch IWO → activate night watch ELINT)

---

[34] Elisa Bertino, Elisa Pierro, Andrea Bonatti, and Elena Ferrari, 21-30.

(RT2) (Activate night watch IWO → activate night watch SIGINT)

(RT3) (Activate day watch IWO → activate day watch ELINT)

(RT4) (Activate day watch IWO → activate day watch SIGINT)

(RT5) (Activate day watch IWO → deactivate night watch ELINT)

(RT6) (Activate day watch IWO → deactivate night watch SIGINT)

(RT7) (Activate night watch IWO → deactivate day watch ELINT)

(RT8) (Activate night watch IWO → deactivate day watch SIGINT after 1hr)

In Role Trigger 8, we have included an example of extending a role for some unforeseen circumstance. For example, if the night IWO wanted to hold the day SIGINT for one hour extra for whatever reason, that could be specified in the activation rules.

The architecture to support the system contains the following data:

1. Active Roles: Table that contains the current active roles.
2. Deferred Actions: Table that contains an entry for each action that may be executed after a certain amount of time.
3. Actions: Table that records the actions that can potentially be executed on Active Roles.
4. Events: Records the activation and deactivation of roles
5. Triggers: Table that contains the specified triggers.

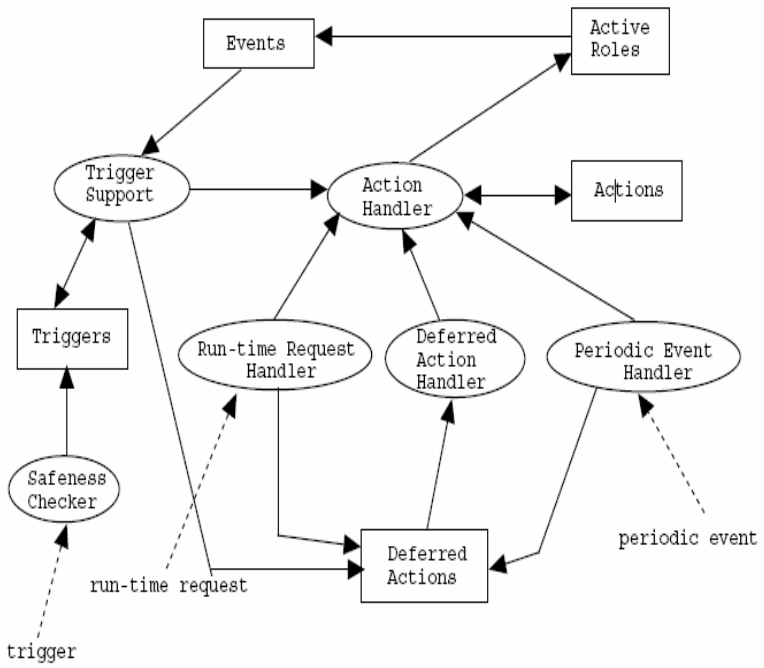

Figure 20. TRBAC Architecture[35]

[35] Elisa Bertino, Elisa Pierro, Andrea Bonatti, and Elena Ferrari, 28.

THIS PAGE INTENTIONALLY LEFT BLANK

V. DISCUSSION

A. RESEARCH RESULTS AND CONTRIBUTIONS

1. Lessons in Model Building

There are many benefits in using varying types of RBAC to build an integrated model. In conducting our research, we found that the base system must have some minimal level of development in order to even start using RBAC models (to modify the base model).

In constructing our model, we further determined that a full integration of CBAC was not necessary or even conducive to achieving our goals. CBAC can be very effective in forming teams (coalitions) to solve a problem or achieve a solution. However, our model is focused on a gradual development of intelligence, only revealing the problem needing a solution very late in the timeline. This makes it virtually impossible to know at the onset which organizations need to be involved and at what level of security.

This made formal use of CBAC in our model prohibitively difficult. Instead, we use our formal model of DRBAC to accomplish any required elements of CBAC. In fact, we view CBAC as a sub-type of DRBAC in the way it uses roles and tasks. Rather than expanding our model to allow us to fully model CBAC, we incorporated the concepts of CBAC under the umbrella of DRBAC.

2. Process for Building a Model

As a result of our research, we found it best to take an incremental approach to applying RBAC principles in order to solve a problem. First, roles are identified and mapped to users. We considered creation of each role in terms of what it needed to accomplish, or data it needed to access. This in turn leads to permission assignments of roles to resource objects (or data within the system). Permissions can be as detailed and granular as required to accomplish the desired task. These permissions should reflect policy as dictated by the parent organiztion.

Once the core concepts of RBAC have been applied, aspects of DRBAC and CBAC can be applied. The DRBAC delegation model must be established to allow the

sharing of data without relying on a central trusted computing base. This is essential in coalition environments where a high level of trust may not exist. Credentail management must be established, whether in the form of DRBAC wallets as discussed in this thesis, or a similar methodology such as PKI.

The process for implementing a RBAC architecture in a coaltion environment requires a basic understanding of the principles of RBAC, TRBAC, and DRBAC. The order in which they should be applied is the same. The first step is to lay the foundation by initializing RBAC:

- The administrator of the system that is going to employ an RBAC architecture should first complete an analysis of the base roles that will be required. This will provide a base building block for implementing furter roles and the addition and deletion of current roles.
- The roles should be identified and given names that correspond to their responsibilites or positions.
- Once the roles have been identified, assign permissions to the base roles. This would also include security labels associated with the roles. The administrator should expect to modify these frequently based on the situation or event.
- The administrator should allow for the introduction of new roles as situations arise.

TRBAC is the next element that is introduced:

- As discussed earlier, triggers should be in place that will activate a base role upon the occurrence of some events or the activation of another role that requires a parallel role.
- TRBAC requires a time element. Expiration dates and times can be included in a role to terminate or extend a role automatically. This

would fall under the umbrella of a trigger, only this trigger would be a time classification trigger.

The final element of coalition RBAC is the implementation of DRBAC.

- DRBAC requires the identification of coalition partners. Base partners should be established and identification of future coaltion partners within the event needs to be analyzed.
- Coalition partners should request the type of access required and this should be approved by the Information Broker authority, who would then set the permissions and assign coaltion roles to existing base roles.
- New roles may need to be established to facilitate the proper access required for a coalition partner depending on where they fall within the Trust Triangle (figure 14).
- "Need to know" criteria should be applied, expecially to non traditional foreign coalition members who may be included during an event specific operation.

The combining of these three will contribute to a seamless exchange of data and information leading to a more efficient coalition environment.

3. Identification of Gaps

In developing the model for this thesis, we have identified two key gaps that require further exporation. The first was mentioned in paragraph 1 above and has aready been discussed, the treatment of CBAC withing DRBAC.

The second gap is our use of a 'black box' Information Broker and requires further research. Without access to a fully functioning Information Broker, we used it as a generic black box concept. We use the Information Broker liberally to share data between roles within or outside of an organization. Radiant Alloy is one potential tool to solve this problem. Full development of Radiant Alloy or the Information Broker concept is outside the scope of this thesis.

4. Integrating RBAC and the Information Broker

The integration of RBAC and the Information Broker concept is a realistic possibility. RBAC requires that there be a controlling entity to provide or deny access to the data or information within a particular data repository. The Information Broker is a logical fit. It acts as a clearing house for requesters and providers of data. If applied to the MDA program, the Information Broker would have to be cleared at the highest level control access using a role based identification system. In essence, the Information Broker will have no idea as to what the actual identity of the person is, just that they are playing a role that requires access to a certain subset of data within a domain. In order to link RBAC and the Information Broker and create a system of systems, there are four items that need to be solved:

1. Identification of roles for a certain event or operation
2. Details of the Information Broker
    a. Centralized
    b. Decentralized
    c. Location
3. Security levels
    a. Data
    b. Roles
4. Time constraint of the operation

If the Information Broker concept can be applied to RBAC, we must examine the possibility of RBAC being applied to the Information Broker and Radiant Alloy. The goal of the Radiant Alloy project is for users to gain access to data across organizational boundaries and across multiple security levels. Role Based Accessed Control along with DRBAC and CBAC can assist in providing a new framework for the Information Broker concept. DRBAC is built for coalition distribution of information and data. The roles that can be created for coalition partners can have set limitations placed on them to control

access to the information that they need to know. The creation of the roles particular to a certain event or operation will be the baseline for controlling the flow of information to coalition organizations or countries. The Information Broker can be the intermediary between the roles and the data, acting as the gateway to the information repository and receiving and filing the data from information providers. This would provide the trusted transactions between users of the information repository (who have been assigned to established roles with established permissions) and providers whose identity would be concealed by the Information Broker.

5. Components and Linkages

The system that is required to support RBAC in a coalition environment is a transaction based system. Additionally, the Information Broker concept has been added to the system structure to assist in the receiving and providing of data (Figure 21). Allowing controlled access to the data within a data repository is the job of an information system. In this case, the access is controlled and the data is distributed by the Information Broker. The information system is modeled using a layered approach and is a hybrid between an information system model and a resource allocation model based on Sommerville's model.[36] The system that would be applied to the MDA program is not a traditional resource allocation system in that the information repository does not contain a fixed amount of data that will eventually run out.[37] But, the data that is contained in the repository is restricted by who it can be delivered to and the users who do have access may be limited by what they can receive.

---

[36] Ian Sommerville. *Software Engineering, Seventh Edition.* (London, England: Pearson Education Limited, 2004), 299-303.

[37] A resource allocation system manages a finite amount of an item. Tickets to a football game or a concert may be managed by a resource allocation system and the users may request the resource (tickets) through the resource allocation system. As tickets are purchased, the system tracks the purchases and reduces the resources available for purchase. The resource does not have to be a tangible object. For example, it can be time such as scheduling classes at a university.

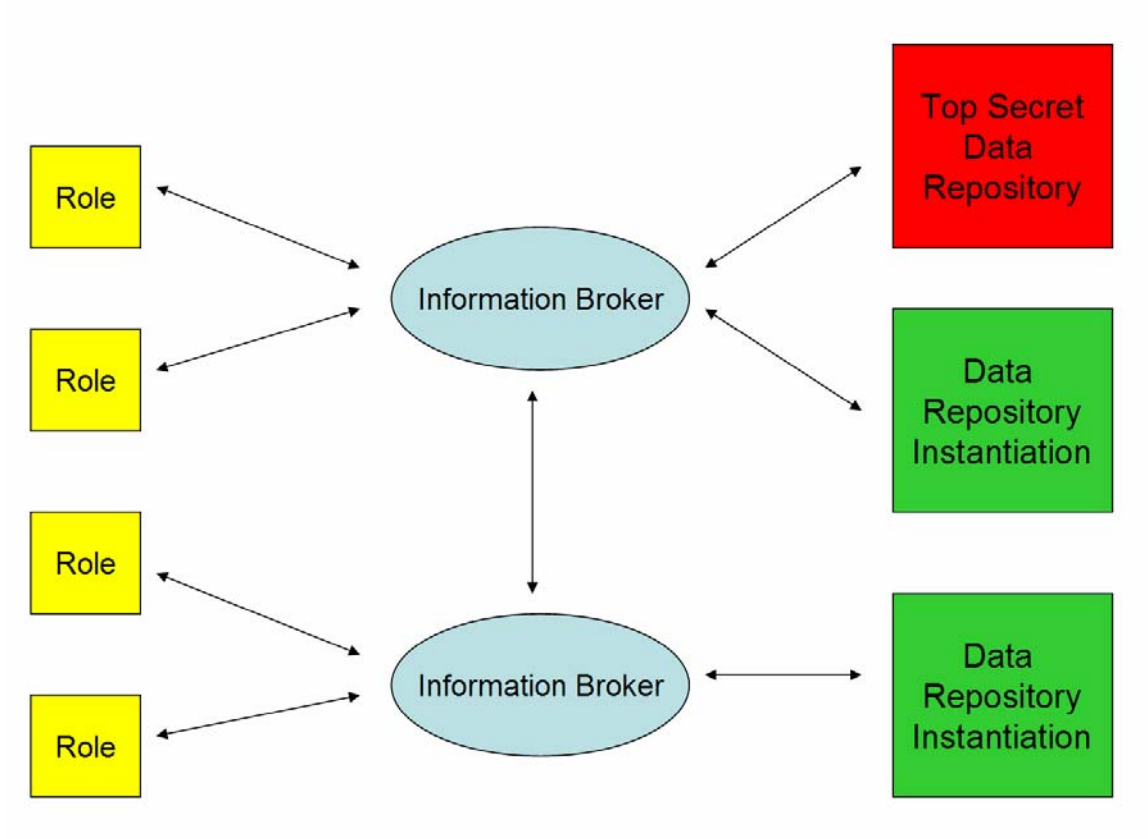

Figure 21. Information Broker as Linkage

The first layer is the user interface layer that provides the mechanism for requesting and displaying the appropriate data. The communication layer is the next layer and that processes the request or distributes the information to the appropriate location within the repository. The third layer is the information retrieval and modification layer which controls, modifies, or updates the data within the information repository. Finally, the fourth layer is the transaction management layer in which the requests are fulfilled.

a. User Interface and Communication Layer

Using Figure 22 as a reference, this model can further be broken down into more detailed components which are explained in the following paragraphs. As an example, the user interface (role) can be a secure connection using a web browser. The user communication layer contains the login verification, request manager, and provider

manager. The login verification would validate the role that is logging in and compare it to time constraints, validity, and clearance level. It employs a rule set that limits who can access what information and for how long. The request manager (Information Broker) deals with queries made by the role player for information or data located within the data repository. This specific request is compared against the security levels of the requested information and data is either provided or denied. The provider manager (data repository) deals with data that is input into the system by information providers (other Information Brokers or data repositories) and it is classified and labeled accordingly. Note from the figure that Information Brokers can access different instantiations of the data repository, but all brokers do not necessarily have access to all the same data repositories. Additionally, brokers can communicate with each other to potentially share data.

b. Information Modification Layer and Transaction Management

The information and modification layer contains application specific components that implement its functionality. Some of these components within the MDA program may include but are not limited to a distributed search, data retrieval, data display, and data logging. These components are linked to the resource data repository which contains the data that is being searched for or requested. The resource data repository is responsible for managing the resources (data) that is contained within it. The distributed search is a search mechanism that looks for the data that the user requested by entering keywords, names, or time constraints into a query. This query management module is linked to the distributed search mechanism and allows the approved user to find the data he or she is looking for. The data retrieval mechanism retrieves the data requested by the user via the resource delivery component. This component prepares the data for delivery to the requestor via the user interface or data display mechanism. Data logging is the final component of the information and modification layer. This is where the accounting takes place and the roles, times, requested data, provided data, and other information is recorded for review. Flags or triggers could be set if there is unusual behavior that may require human intervention to ensure that no security break has taken

place. The transaction management layer coordinates the transactions between the user and the Information Broker, providing the data immediately or informing the user of delays and expected time of the delivery of the data.

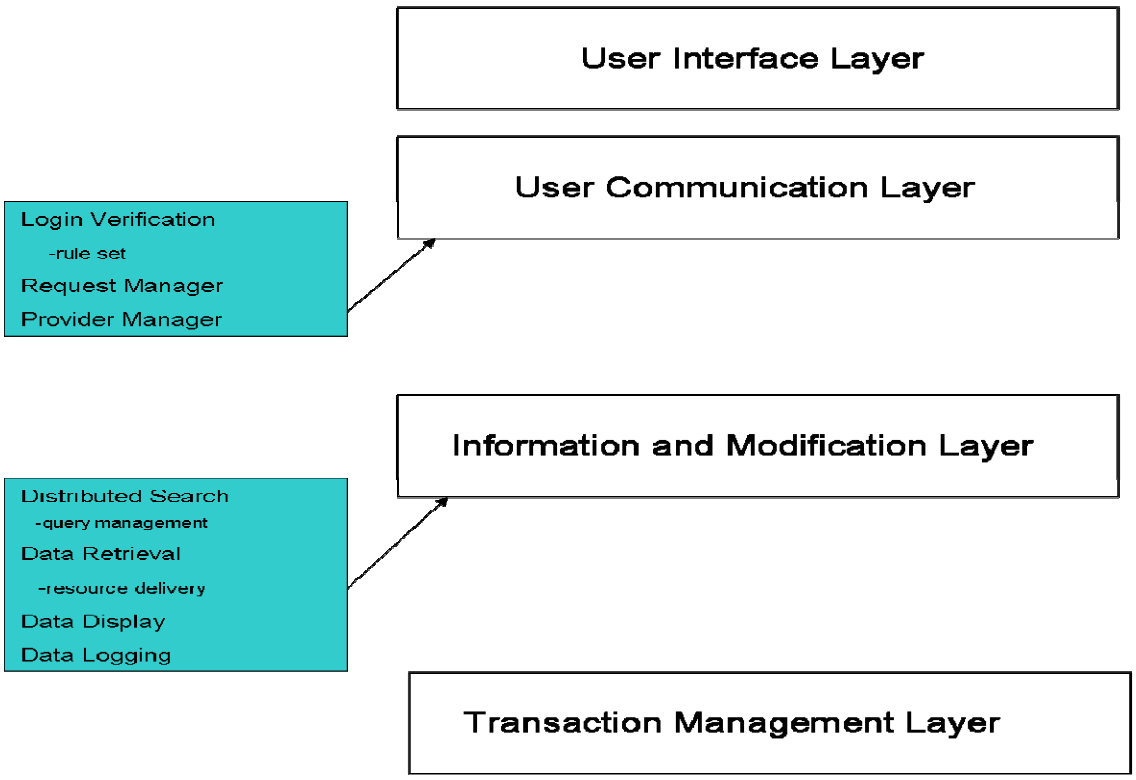

Figure 22. Information and Resource Management

VI. CONCLUSION AND FUTURE RESEARCH

A. SUMMARY

The purpose of this research is to help solve a problem, which is, how we can best achieve Shared Situational Awareness (SSA) among coalition partners in order to accomplish joint missions. As discussed earlier, coalitions may be very diverse and may include both foreign and domestic militaries, law enforcement, intelligence agencies, as well as private industry. We have investigated the capabilities and limitations of Role-Based Access Control (RBAC) to control the dissemination of SSA in this environment.

Through developing case studies, we found RBAC to be a useful tool in sharing information between coalition members. The chief negative aspect to using RBAC is the initial overhead involved in establishing the roles and permissions. If this initial hurdle can be overcome, maintaining the system is quite simple. Users need only be assigned roles to attain immediate access to needed information.

Similarly, DRBAC (and CBAC) provided a useful mechanism to scale the sharing of information without having to rely on a central trusted computing base. DRBAC wallets provided the capability to publish, validate, update and revoke delegations. Wallets function similar to PKI certificates and stored many delegations. TRBAC allowed the use of time based triggers and restrictions to be placed on roles. This is especially important in cases where you may want coalition members to access sensitive data on a temporary basis. TRBAC allows you to activate and deactivate roles in a manner that accomplishes this.

Our main purpose was to model case studies in which RBAC could possibly be applied. We focused on the MIFC examples to determine the feasibility of applying RBAC to events that include coalitions internal to the United States and external non traditional allies. We determined that RBAC in conjunction with DRBAC and TRBAC could be feasible and beneficial to assisting the MDA program in working with coalitions. Additionally, there may be the potential for RBAC to be applied to the Radiant Alloy program in order to achieve their goal of Protection Level 5. Roles could be used instead of standard users to help simplify the process.

The interlinking between RBAC, Information Broker, and Radiant Alloy is technically possible. The elements of DRBAC and CBAC are most appropriate to align with the Information Broker, especially when designing a system for coalition use. It is scalable to large data sets and can include large quantities of entities and roles. DRBAC is especially useful for coalition environments and can limit information to members that have lower clearances or when combined with an information broker, it can also prevent knowledge of the source of the data which is equally important.

B. RECOMENDATIONS FOR FUTURE RESEARCH

As suggested in this research, the implementation of RBAC in actual systems has been realized with some success. By all indications, this research is a first step towards development of an information sharing system capable of supporting large and diverse coalitions. There are many different converging paths that future researchers might study to contribute to solving the Shared Situational Awareness problem. We offer three recommendations for future research in this area.

1. Extending the Model

The first and most obvious area for future research would be to simply extend the model. Out of necessity, the models and case studies developed here were of limited scope. These models could be expanded by using them as a baseline for constructing and implementing an architecture.

2. Attribute Based Access Control

Another related area that deserves further examination is the use of Attribute Based Access Controls (ABAC). ABAC grants accesses to services based on the attributes possessed by the requester.[38] ABAC is different from traditional DAC because it replaces the *subject* by a set of attributes and the *object* by a set of services in the access control matrix. This is useful in systems in which subjects (roles) are identified by

---

[38] L. Wang, D. Wijesekera, and S. Jajodia. *A Logic Based Framework for Attribute Based Access Control.* In Procedure Workshop on Formal Methods in Security Engineering. (New York: ACM Press, October 2004), 45-55.

their characteristics, such as those substantiated by DRBAC wallets. These can be modeled as attribute sets. The model uses logic programming with set constraints to accomplish access control.[39]

3. Information Brokers

The Information Broker plays an important role in our concept. Information Brokers fulfill a need by collecting and distributing assets to consumers or users of information.The Information Broker creates value in the form of time and place. It can deliver the asset (data) at the time it is desired and to the place it is required. [40] When the Information Broker concept is applied to MDA, it can provide a positive benefit.

The Information Broker concept provides two possible modes for distirbution of data. The first is strictly as an intermediary, which we have used extensively in our modeling of the problem. In this mode, the user (assigned to a role) requests data and the Information Broker determines the access level, acquires the data, and returns it to the user assuming all security checks have been passed. The second and most probable mode of delivery is the automatic piping mode. This method allows an existing role to have data automatically piped to them as an event changes. This relieves the user of having to request data on a continuous basis. This mode of delivery would be an excellent addition to the model and developing an automatic piping system is an excellent area for future resarch and development.

---

[39]Wang et al., 45-55.

[40]Wayne C. Lim. Managing Software Reuse. A Comprehensive Guide to Strategically Reengineering the Organization for Reusable Components. (Upper Saddle River, NJ: Prentice Hall PTR, 1997).

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX GLOSSARY

Actor - An actor is any individual or group participating in a specific activity related to the current operation

Coalition - A group working together toward a common goal, but may not have a high level of trust.

Coalition Based Access Control (CBAC) - An access control method that is a derivative of RBAC and used in conjunction with a DRBAC policy to support coalition access control policies.

Consumer - Users of information or data that is stored within an information repository.

Credential – Used with DRBAC, a subset of access permissions that establishes the identity of a user. Generally, a biometric, user id, password, or some other verification technique is used to establish identity.

Delegation – In DRBAC, the term is used to describe passing on authority or permissions to access certain data.

Distributed Role Based Access Control (DRBAC) - An access control method that is a derivative of RBAC and is used for systems that span multiple domains. It is also used to control access in a coalition environment.

Entity – In DRBAC, the term is used to describe either resources or principals and have a unique PKI public identity.

Information Broker – Used in the Radiant Alloy concept of operations, the Information Broker is an information-management service that acts as an intermediary between the requester of the information and the data repository. The IB will provide the requester with the data and at the same time, shield the source of that data from the requester.

Non Government Organization (NGO) – Organizations who are not a part of any government and generally operated in a not for profit capacity and work to further the political or social goals of their members.

Permissions (privileges) – Authorizations to perform some action on the system.

Producer – Providers of information or data to the information repository.

Radiant Alloy – Department of Defense effort to develop solutions to exchanging data and information across security levels and domains

Role – A collection of permissions for a user who is assigned to a specific task and filling a predetermined position (or role)

Role Based Access Control (RBAC) - A method of access control in which permissions are assigned to roles and users are made members of these roles.

Shared Situational Awareness – Information sharing across domains and organization in which the players all have access to the same data in order to make informed decisions.

Temporal Role Based Access Control (TRBAC) – Used to track the dynamic aspects of RBAC that includes the periodic activation and deactivation of roles over time.

User – Individuals who interface with a computer. Users receive permissions only through the roles in which they are assigned.

Valued Attribute – In DRBAC, a valued attribute allows for control of access rights and supports different levels of access for the same resource.

Wallet – A local or non-local stored profile of a role that contains access and privilege information.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Agar, Chris, Kevin Smith, and Troy Wright. *Role Based Access Control*. PowerPoint Presentation, April 18, 1998.

Athans, Michael. *The Expert Team of Experts Approach to Command and Control Organizations.* Control Systems Magazine. September 1982, pp. 31-37.

Athans, Michael. *Command and Control Theory: A Challenge to Control Science.* IEEE Transactions on Automatic Control, VOL AC-32, NO.4. April 1987, pp. 286-293.

Bennett, Lieutenant Michael E. *Defining a Common Intelligence Picture for the United States Coast Guard: A Port Perspective.* Joint Military Intelligence College, August, 2003.

Bertino, Elisa, Elena Ferrari, and Evaggelia Pitoura. *An Access Control Mechanism for Large Scale Data Dissemination Systems.* Eleventh International Workshop on Research Issues on Data Engineering, 1-2 April 2001, pp 43-50.

Bertino, Elisa, Elisa Pierro, Andrea Bonatti, and Elena Ferrari. *TRBAC: A Temporal Role Based Access Control Model. Department of Computer Science.* Symposium on Access Control Models and Technologies. Berlin, Germany: ACM Press, 2000, p 21-30.

Castano, Silvana, Maraigrazia Fugini, Giancarlo Martella, and Pierangela Samarati. *Database Security*. ACM Press, 1995.

Cebrowski, Vice Admiral Arthur K. and John J. Garstka. *Network-Centric Warfare: Its Origin and Future.* Proceedings of the Naval Institute. January, 1998. Available from: <http://www.usni.org/Proceedings/Articles98/PROcebrowski.htm> (accessed on 12 October 2004).

Chandramouli, Ramaswamy, David F.Ferraiolo, Serban Gavrila, D. Richard Kuhn, and Ravi Sandhu. *Proposed NIST Standard for Role Based Access Control.* ACM Transactions on Information and Systems Security. Volume 4, Issue 3. New York: ACM Press, August 2001.

Chandramouli, Ramaswamy, and Ravi Sandhu. *Role Based Access Control Features in Commercial Database Management Systems.* National Information Systems Security Conference. Crystal City, VA: October 6-9, 1998.

Cohen, E., R. K. Thomas, W. Winsborough, and D. Shands. *Models for Coalition-Based Access Control (CBAC).* Proceedings of the Seventh ACM symposium on Access Control Models and Technologies. Monterey, CA: ACM Press, 2002, p. 97-106.

Collins, Vice Admiral Thomas H. United States Naval Institute Speech. April 3, 2002. Available from: <http://www.uscg.mil/COMMANDANT/Maritime%20Security%20Plan%20USNI%20040302.htm> (accessed 19 September 2004).

Coyle, Karen. *Rights Expression Languages: A Report for the Library of Congress.* February 2004.

Director of Central Intelligence Directive 6/3. *Protecting Sensitive Compartmented Information Within Information Systems.* June 1999.

Ferraiolo, David F., D. Richard Kuhn, and Ramaswamy Chandramouli. *Role Based Access Control.* Norwood, MA: 2003.

Ferraiolo, David F., D. Richard Kuhn. *Future Directions in Role Based Access Contol.* Symposium of Access Control Models and Technologies. Gaithersburg, MD: 1996.

Ferraiolo, David F., D. Richard Kuhn. *Role Based Access Control.* National Institute of Standards and Technology. Gaithersburg, MD: 1992.

Ferraiolo, David F. *An Argument for the Role Based Access Control Model.* ACM Workshop on Role Based Access Control. Chantilly, VA: ACM Press, 2001.

Freudentahl, Eric, Tracy Pesin, Lawrence Port, Edward Keenan, and Vijay Karamcheti. *DRBAC: Distributed Role-based Access Control for Dynamic Coalition Environments.* 22nd International Conference on Distributed Computing Systems. Vienna, Austria: 2-5 July 2002, pp 411-420.

Johns Hopkins University Applied Physics Laboratory Web Site. Available from <http://www.jhuapl.edu/newscenter/aplnews/2004/summer_MDA.htm> (accessed 19 September 2004).

Khayat, Etienne and Nimal Nissanke. *Risk Based Security Analysis of Permissions in RBAC.* Center for Applied Formal Methods, London South Bank University. London, England: 2004.

Kuhn, D. Richard. *Mutual Exclusion of Roles as a Means of Implementing Separation of Duty in Role-Based Access Control Systems.* Second ACM Workshop on Role Based Access Control, Gaithersburg, MD: ACM Press, 1997.

Kuhn, D. Richard. *Role Based Access Control on MLS Systems Without Kernel Changes.* Proceedings of the Third ACM Workshop on Role-based Access Control. Fairfax, Virginia: ACM Press, 1998.

Lim, Wayne C. *Managing Software Reuse. A Comprehensive Guide to Strategically Reengineering the Organization for Reusable Components.* Upper Saddle River, NJ: Prentice Hall PTR, 1997.

Lupo, Emil C. and Jonathon D. Moffett. *The Use of Role Hierarchies in Access Control.* Symposium on Access Control Models and Technologies. Fairfax, VA:1999.

Sandhu, Ravi S, Edward J. Coyne, Hal L. Feinstein, and Charles E. Youman. *Role Based Access Control Models.* IEEE Computer, Volume 29, Number 2. IEEE Publishing, February 1996, pp. 38-47.

Sommerville, Ian. *Software Engineering, Seventh Edition.* Pearson Education Limited. London, England: 2004.

Wang, L. D. Wijesekera, and S. Jajodia. *A Logic Based Framework for Attribute Based Access Control.* In Procedure Workshop on Formal Methods in Security Engineering. New York: ACM Press, October 2004, pp. 45-55.

Wikipedia.org <http://en.wikipedia.org/wiki/Non-governmental_organization> (accessed 12 April 2005).

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Professor Bret Michael
   Naval Postgraduate School
   Monterey, California

4. Professor Alan Ross
   Naval Postgraduate School
   Monterey, California

5. Captain Steven Ashby
   Naval Postgraduate School
   Monterey, California

6. Fred Glaezer
   Navy TENCAP (Maxim Corp)
   Monterey, California

7. Prof Hersch Loomis
   Naval Postgraduate School
   Monterey, California

8. Scott Blatter
   MIFC
   Alameda, California

9. LT Michael Bennett
   MIFC
   Alameda, California

10. Curtis Enge
    Northrop Grumman
    San Diego, California

11. Chris Newcomb
TENCAP West
San Diego, California

12. Stan Kowalsky
SAIC/SPAWAR
San Diego, California

13. Debbie Blais
SAIC/SPAWAR
San Diego, California

14. Cathy Zhang
Northrop Grumman
San Diego, California

15. Thuy Ton
Northrop Grumman
San Diego, California

16. Jeff Wagner
Northrop Grumman
San Diego, California

17. Gerald Brown
Navy TENCAP (Maxim Corp)
San Diego, California

18. Professor Duminda Wijesekera
George Mason University
Fairfax, Virginia